Exploring Undergraduate Interactions with Mobile Privacy and Security

Sarina Till

December 2018

Contents

1 Introduction **1**

2 Literature Review **5**

3 Methods **15**

3.1 Understanding of Permissions and Security 16

3.1.1 Description of Mobile Applications used 16

3.1.2 Types of questions asked 20

3.2 Survey 20

3.3 Inclusion of Deception 22

3.4 Observation 23

3.4.1 Observation Process 24

3.5 Interviews 25

3.6 Debriefing and closing of observations and Interviews 25

3.7 Data Analysis 26

3.7.1 Qualitative Data Analysis 26

3.7.2 Quantitative Data Analysis 26

3.8 Limitations of the Study 27

4 Findings **29**

4.1 Understanding of Permissions and Security 29

4.1.1 Students do not pay attention to application permissions when they install applications. 29

4.1.2 Students do not pay attention to run time permissions - even when they believe they do. 31

4.1.3 Students have become desensitised to permissions that are often requested. 32

4.1.4 Students are not aware that applications make use of more permissions than the explicitly requested permissions. 34

4.2 Technical Ability with regards to permissions and privacy 35

4.2.1 Students do not match the permissions requested to the functionality of the application. 35

4.2.2 Students do not know where to check what permissions applications are using. 37

4.2.3 Students do not notice if updates change mobile permissions. 37

4.3 Student Understanding of Location-Based Services 38

4.3.1 Students believe they consider location services, however, the data shows that they do not. 38

4.3.2 Students are not sure how location tracking services works. . 39

4.4 Understanding of encryption as a security measure 40

4.4.1 Students do not know what encryption is nor do they recognise encryption symbols. 40

4.5 Overall student competency in terms of mobile permissions, encryption and location-based services 42

5 Characterising digital natives' approaches to mobile privacy and security **44**

5.1 Digital natives lack the necessary technical skills to engage with mobile privacy and security. 45
5.2 Digital natives do not understand mobile and privacy features and therefore ignore them. 46
5.3 Digital natives have been overexposed to application requests that violate their privacy and have become desensitised. 49
5.4 Digital natives trust the authors of software and fail to act securely when security and privacy features are requested out of context. . 49
5.5 Digital natives' need for instant gratification has consequences for privacy and security. 51
5.6 Digital natives' definition of privacy is different than those of previous generations. 52

6 Conclusions and Future work **54**

6.1 Appendixes 66
6.1.1 Survey 66
6.1.2 Interview Script 78
6.1.3 Informed Consent Form 80

List of Figures

3.1 Screenshot of the VCChatter app used during interviews and for the survey. This basic text-only app over-requested permissions and was not encrypted. 17
3.2 Screenshot of the VCCanteenRater app used during interviews and for the survey. This app allowed students to rate the university canteen, and over-requested permissions. 17

4.1 Survey question testing both the the presence and lack of encryption. 41
4.2 Example of WhatsApp using both an encryption icon and a short message to indicated the presence of encryption. 42

5.1 Phone Permission Group Rationale. 48
5.2 Similar Messenger Application Icons with Different Authors on the Google Play Store. 50
5.3 Actual Facebook Messenger App. 50

List of Tables

2.1 Android permissions and protection levels 14

4.1 Students displaying inconsistent encryption related answers 40

5.1 Android Phone Permission Group 47

Abstract

Many studies have proven that digital natives are not as tech-savvy as previously thought, and possibly vulnerable in terms of privacy and security. My focus was to characterise how this generation interacted with mobile privacy and security. We provide evidence from a cohort of South African students, using this to discuss areas in which they need to be protected. We employed a web-based survey of 77 students, supplemented by in-depth interviews with 10 additional students. In both cases, we enquired about knowledge of permissions, encryption and application installation practices. With the in-depth interviews we also observed students as they installed two applications, one of which over-requested permissions. Our findings showed that most students (80%) did not look for- or understand permissions, did not understand or look for encryption, and used location-based services unsafely. Based on these results, we argue that digital natives lack the technical skills to properly engage with mobile privacy and security. Furthermore, digital natives do not understand mobile security and privacy features and therefore ignore them. Digital natives trust the authors of software and fail to act securely when security and privacy features are requested out of context. We further argue that this generation of digital natives has been so overexposed to mobile requests that violate their privacy and security that they have become desensitised to them. We further argue that digital natives' definition of privacy is different from that of previous generations. Lastly, we discuss the implications of our findings for Higher Education Institutions, Higher Education Policy and mobile application design.

Chapter 1

Introduction

South African Higher Education is in a process of reform and restructuring. This process serves not only to redress the past, but also to move South Africa closer to a knowledge economy [CHE, 2018]. Part of this process is the drive to include ICT in the Higher Education sector. This movement is driven by government policies such as: The National Development Plan, the National Development Plan for Higher Education and The National Research Development Strategy. All of these documents speak to the need for Higher Education to adopt ICT in order to deliver graduates who are equipped with 21st Century skills to join the Knowledge Economy [CHE, 2018].

In response to this movement, Higher Education Institutions have seen a particularly large growth in mobile phone usage on their networks. According to Porter et al [Porter et al., 2014] more and more Higher Education Institutions are implementing blended learning using popular Learning Management Systems such as Blackboard. To ensure accessibility to these systems, institutions often offer free WiFi to their student bodies. These students access networks, learning mate-

rial and institutional content on their mobile phones through a mobile application often provided by the developers of the LMS.

To further complicate the matter, most students currently enrolled in these institutions were born in the digital age and are often referred to as digital natives or the net generation. Barak [Barak, 2018] describes these students as immersed in technology, more tech-savvy than the generations before them and well versed in the online world. In fact, these students are believed to have changed so much that their entire learning style has changed and education needs to be readjusted to keep up.

Despite this, Kurkovsky and Sytya's 2010 study *Digital Natives and Mobile Phones* [Kurkovsky and Syta, 2010] found that digital natives are not technologically advanced, lack knowledge regarding privacy and security and often downplay the risks of using mobile phones. I argue that while education may need to be readjusted, the digital proficiency of these students may still be over-estimated, particularly in their awareness and perception of security and privacy. Later works by Bullen Morgan [Bullen and Morgan, 2016] and Gkioulos et al [Gkioulos et al., 2017] indicate that Kurkovsky's 2010 findings are still valid today. Both sets of authors argue that while digital natives might interact with technology differently than previous generations, there is little evidence that they are more tech-savvy or have a better understanding of privacy and security.

This lack of "tech-savvyness" combined with the drive for ICT in Higher Education Institutions in South Africa, which in turn leads to the en masse uptake of mobile technology, poses very real implications for both the design of mobile security as well as Higher Education Institutions. In order to further investigate

this, I surveyed 77 students and conducted in-depth interviews with 10 students at a premier private undergraduate university in South Africa.

I tested the interactions of these digital natives with Android-based mobile application permissions, location-based services and encryption technologies in an effort to understand how these students interacted with these mobile privacy and security features. I found that students act insecurely, do not understand mobile permissions or encryption, and are possibly not ready to safely use the technology being pushed onto them. This finding is further aggravated by the anecdotal belief that digital natives cope better with all aspects of technology. In this paper I present the results as well as the implications for the design of Android's mobile security. I also present the implications for educational institutions who prescribe technology in their teaching and, in turn, drive the uptake of mobile devices.

My work marks the following two contributions to the CHI community. Firstly I provide a characterisation of how digital natives currently interact with mobile privacy and security. Secondly I highlight the fact there is currently little in the way of government policy in terms of the governance of ICT in Higher Education Institutions. Thirdly, I highlight the fact that most Higher Educational Institutions are only partially ready to adopt ICT with privacy and security as one of the major areas for concern.

Considering the contributions above, I am suggesting that there is a need to better educate our youth about mobile app use through a coordinated program to be offered in Higher Education Institutions, and to rethink our approach to usable mobile privacy and security.

Next, I discuss the literature in terms of: The uptake of ICT and, in turn, mobile devices in South African Higher Education Institutions, followed by the vulnerabilities of Android privacy and security, Android's security features, and

usability recommendations, and, lastly, the lack of training and support for good privacy and security behaviours in South African Higher Education Institutions.

Chapter 2

Literature Review

The convenience of next-generation devices has led to the surge in the use of these devices in Higher Education Institutions (HEIs) [Miller et al., 2012]; these devices fill needs such as blended and online learning as well as reaching ever-growing student bodies [Rambe and Bere, 2013, Mtega et al., 2012]. This is especially true in the South African context where in line with government policy, eighty nine percent (89%) of South African institutions make use of a BOYT (Bring Your Own Technology) policy to harness the prospects of blended and m-learning in order to provide democratic access to learning [De Kock and Futcher, 2016, Rambe and Bere, 2013, Mtega et al., 2012]. Of these devices, Android is the most popular mobile operating system at present with over 70% [Tang et al., 2017] of the market share. Unfortunately, the open source nature of this operating system also makes it the most likely to be attacked by malware and grayware. In fact, ten percent of global attacks occurred in the education sector over the last seven years, and 87% of mobile attacks were Android-based. These attacks aim to install adware, trojans and rootkits as well as spy on users, steal information and so forth. This operating system is also more prone to zero-day attacks, which

can cause confidentiality and integrity breaches. [Lin et al., 2012, Du et al., 2017, Santhanam et al., 2017].

Mobile devices are infected by malware either by attackers finding and exploiting vulnerabilities in the form of zero-days, or by users being tricked into installing malicious applications [Khandelwal and Mohapatra, 2015]. The malware is then able to exploit users' private information which could have devastating consequences. Android offers a permissions-based model aimed at protecting users and their privacy [Android, 2018b]. The permissions are classified into three broad protection levels known as, *normal*, *signature* and *dangerous* permissions. Android states that normal permissions pose minimal risk to a user's privacy and security and are therefore automatically granted upon the installation of the application[Android, 2018b]. For example, if a mobile application requires access to the internet, the INTERNET permission should be listed in the application's Android Manifest file (AndroidManifest.xml). If the permission is present, the application will be able to access the internet through the mobile phone's hardware. If the permissions are not present, the application will simply not work, or throw a security exception.

Signature permissions are also granted at install time, but only if the application is signed by the same certificate as the application that defines the permissions. For example, if you have a running application and a calendar application developed by the same company, it is possible for these two applications to communicate. You might want to set a reminder for your next run that includes the distance and time of your last run. Signature permissions makes it possible for applications to share data and permissions as long as the applications were signed by the same certificate, and are developed by the same company. The user is therefore not

asked to allow the ACCESS_CALENDAR permission again, as the running app will get the permission from the already installed calendar app.

Permissions that fall under the dangerous category need explicit consent from a user in order to access information such as their calendar, contacts, photos, files and location, as these permissions could affect users' privacy and security. Depending on the API (Application Programming Interface) of the device, users are presented with a list of the required permissions either before they install the application, or at run time (when a feature which requires a permission is first accessed by the user) [Android, 2018b]. Users are then tasked with deciding whether they wish to install or use the application. For example: if an application needed to access the mobile phone's GPS system, it would need to contain the ACCESS_COARSE_LOCATION and or the ACCESS_FINE_LOCATION permission in its Android Manifest file (AndroidManifest.xml). Having these permissions in the file and requesting the permission from the user at run time enables the application to access the permission-protected GPS system through an Android API call. Should the application not contain the required permissions in the Manifest file, or if the permission has not been previously allowed, any request to a permission protected resource will also result in the Android operating system throwing a security exception or simply not allowing the process. Users can selectively allow access to resources that could affect their privacy by allowing or denying *dangerous* permissions if they are using API 24 (Marshmallow) and above [Johnson et al., 2012]. Once the application is installed, only the dangerous permissions can be toggled on and off. Signature and Normal permissions remain static and are not changeable. A list of the permissions in each category is detailed in table 2.1.

Permissions also tend to change when applications are updated. Application

updates and permission updates requested by applications are treated differently on different API Levels. Prior to Lollipop (API 22), users needed to give explicit access to each permission that changed with new updates. However, from Lollipop onward, permissions are automatically allowed if the user has automatic updates enabled [Developer Admin, 2014].

Android's permission model comes with shortcomings of its own. The model is too coarse [Tang et al., 2017], places too much responsibility on the user, uses no sandboxing and an open market [Singh et al., 2016]. Applications also often make use of more permissions than explicitly disclosed to the user [Barn et al., 2014].

Whilst Android has features which allow users to encrypt data on their handsets, Android itself has very limited security [Ongtang et al., 2010]. Application developers are tasked with the inclusion of security features such as encryption [Mylonas et al., 2013]. The sophistication of mobile phones and the multimodal nature of messages sent from these phones makes it crucial to include encryption of mobile transmissions and local data on the mobile device itself, as well as provide firewalls [Lin et al., 2012]. Sadly users do not normally enable the encryption services [Mylonas et al., 2013], available to them.

Location tracking also poses serious privacy and security risks to mobile users. Many platforms, such as Google's universal analytics and Facebook's conversion pixel, provide location-tracking data to customers to better target advertising [Arp et al., 2017]. LBS (location-based services) can provide a very good estimate of a user's physical location. These services are normally used for services such as navigation, or to pinpoint nearby needed locations such as ATMs. However, these devices raise privacy and security control questions because the user

has little or no control regarding which information is shared. This information can, and has, been accessed by attackers or third parties [Rao and Girme, 2015]. Many mobile applications require constant tracking of user locations in order to function. LBS such as navigation and Facebook's Nearby Friends do not only track, but also publish mobile end users' physical locations. Location tracking reveals intimate details regarding a user's daily routine and poses a significant risk. Not only can mobile phones be used to track user locations, they can also be used to predict their next location based on previous data. This fact becomes evident when one downloads one's own Google location timeline which creates a map that shows all the locations you have visited and when [Zhu et al., 2013]. It is very easy to derive user patterns from here. Combining location tracking with maps and GPS coordinates can lead attackers straight to an LBS user [Li et al., 2006].

Users are often the weakest link in any security system [Li and Clark, 2013]. In line with this, previous works have indicated that users do not understand mobile permissions [Kelley et al., 2012] and therefore tend to ignore them [Imgraben et al., 2014]. Users further tend to be neglectful when it comes to security features [Mylonas et al., 2013, Imgraben et al., 2014] and do not use these optimally or at all. This behaviour can be attributed to the fact that users are unaware of the possible dangers that lurk on their mobile devices, nor are they aware of the value of their personal data.

It also speaks to the usability of security features. Good security is only possible if it is designed with good usability in mind. There is surprisingly little work done on the usability of mobile privacy and security features [Quay-de la Vallee et al., 2016]. End users often resort to reading the comments and reviews of mobile applications to find out how secure and safe the application is to use [Tang et al., 2017]. BYOT (Bring Your Own Technology) has allowed devices to connect to current infrastructure en masse. This, in turn, has created an unprecedented security landscape

which is incredibly hard to navigate [Imgraben et al., 2014]. Given the fact that users and their interactions with privacy and security directly impacts on the effectiveness of these features, I discuss the criteria for security and privacy features with good usability next.

The tension between usability and security is well understood. It is generally accepted that even the best security feature is likely to fail if it does not consider the users who interact with it [Dhillon et al., 2016]. The following methods have traditionally been used to measure usability in security [Birge, 2009]:

- Usability and Design Studies: which employ traditional usability methods to evaluate mainly user interfaces.
- Security Feature Studies: which focuses on evaluating the usability of security features that do not directly involve the user. This touches on areas such as database encryption, cryptographic protocols etc.
- Trust and Ethical Studies: These studies focus on ethical concepts such as trust, privacy, legality, morality and diversity.
- Security and Privacy Experiences: These are more recent studies that focus on users' experiences, attitudes and concerns regarding security and privacy.
- Modelling & Guidelines: These studies are aimed at creating models and guidelines to include usability in security.

Later works placed a strong emphasis on the importance of Human Computer Integration and advocated for security that focuses on the human aspect of computing [Mylonas et al., 2013]. These studies argue that good, highly usable security should meet the following requirements [Mylonas et al., 2013, **?**, Hanus and Wu, 2016]:

- Promoting user understanding.

- Preventing incorrect and insecure actions by users.
- Scaffolding of security and usability.
- Empowering users.
- Not forcing users to jump through unnecessary hoops.
- Efficient use of user attention.
- Empowering users to make informed decisions.
- Consistency
- Security as a default to create a consistent fearless system.

The above-mentioned methods and criteria go a long way towards offering more usable security systems, however, a deeper look at user behaviour is necessary [Wang et al., 2017]. For example, the rationale users give for adopting security features should be considered. In line with this, the expectations of users, as well as the context in which users are experiencing security features should also be included in security designs [Sarma et al., 2012]. Lin, Amini and Hon [Lin et al., 2012] found that many users will deny or allow security based on their current context as well as what users expect from software. For example, users are much more likely to allow security exceptions for a feature they expect would need it, such as a chat application requesting access to a user's contact list, versus a rating application doing so. Good usability should also consider the fact that not all users are created equal. There is a big difference between the adoption of security features in the first and third world [Ahmed et al., 2016]. Western security is designed for western views - users from other regions may not experience or use the security in the intended manner [Dunphy et al., 2014].

Even though there has been a mass uptake of technology in Higher Education Institutions in South Africa, little attention has been paid to the effect this may have on institutional policy. The Council for Higher Education (CHE) makes mention of the lack of a coordinated policy to govern ICT in Higher Education Institutions. This is echoed by Jaffer et al [Jaffer et al., 2007] who states that no coordinated policy exists at government or institutional level. Czerniewicz et al [Czerniewicz et al., 2006] further explains that Higher Education ICT policy in South Africa is an emerging field of enquiry that has not enjoyed as much attention as it has in other countries, such as Canada and England.

Ruxwana and Msibi [Ruxwana and Msibi, 2018] found that most South African HEIs are only partially ready for the adoption of a BYOD approach, with end user education in terms of privacy and security as one of their main areas of concern. In line with Ruwana and Msisibi, Chin et al [Chin et al., 2016] argues for a fit for purpose and effective training program that would assist students with the safe and secure use of mobile devices on campuses.

The Android Permissions system has shortcomings and does not enjoy high levels of usability paired with the fact that users often act insecurely regardless of the security measures available to them. One needs to consider the fact that we currently lack government policy to govern the adoption of ICT in Higher Education Institutions. Further to this HEIs are only partially ready to adopt a BYOD approach. These very institutions are currently experiencing an en mass uptake of mobile devices to aid access to learning. It has now become increasingly critical that we understand how student bodies interact with mobile privacy and security in order to prepare and safeguard them.

As I am interested in the behaviour of digital natives and their interaction with

mobile security and privacy features in the education sector, I embarked on the study detailed in Chapter 3 and the remainder of this thesis. Below, I detail my findings followed by a discussion of the findings, and lastly I provide my conclusions and recommendations for future work.

Normal Permissions	Signature Permissions	Dangerous Permissions
ACCESS_LOCATION_EXTRA_COMMANDS	BIND_ACCESSIBILITY_SERVICE	READ_CALENDAR
ACCESS_NETWORK_STATE	BIND_AUTOFILL_SERVICE	WRITE_CALENDAR
ACCESS_NOTIFICATION_POLICY	BIND_CARRIER_SERVICES	READ_CALL_LOG
ACCESS_WIFI_STATE	BIND_CHOOSER_TARGET_SERVICE	WRITE_CALL_LOG
BLUETOOTH	BIND_CONDITION_PROVIDER_SERVICE	PROCESS_OUTGOING_CALLS
BLUETOOTH_ADMIN	BIND_DEVICE_ADMIN	CAMERA
BROADCAST_STICKY	BIND_DREAM_SERVICE	READ_CONTACTS
CHANGE_NETWORK_STATE	BIND_INCALL_SERVICE	WRITE_CONTACTS
CHANGE_WIFI_MULTICAST_STATE	BIND_INPUT_METHOD	GET_ACCOUNTS
CHANGE_WIFI_STATE	BIND_MIDI_DEVICE_SERVICE	ACCESS_FINE_LOCATION
DISABLE_KEYGUARD	BIND_NFC_SERVICE	ACCESS_COARSE_LOCATION
EXPAND_STATUS_BAR	BIND_NOTIFICATION_LISTENER_SERVICE	RECORD_AUDIO
FOREGROUND_SERVICE	BIND_PRINT_SERVICE	READ_PHONE_STATE
GET_PACKAGE_SIZE	BIND_SCREENING_SERVICE	READ_PHONE_NUMBERS
INSTALL_SHORTCUT	BIND_TELECOM_CONNECTION_SERVICE	CALL_PHONE
INTERNET	BIND_TEXT_SERVICE	ANSWER_PHONE_CALLS
KILL_BACKGROUND_PROCESSES	BIND_TV_INPUT	ADD_VOICEMAIL
MANAGE_OWN_CALLS	BIND_VISUAL_VOICEMAIL_SERVICE	USE_SIP
MODIFY_AUDIO_SETTINGS	BIND_VOICE_INTERACTION	BODY_SENSORS
NFC	BIND_VPN_SERVICE	SEND_SMS
READ_SYNC_SETTINGS	BIND_VR_LISTENER_SERVICE	RECEIVE_SMS
READ_SYNC_STATS	BIND_WALLPAPER	READ_SMS
RECEIVE_BOOT_COMPLETED	CLEAR_APP_CACHE	RECEIVE_WAP_PUSH
REORDER_TASKS	MANAGE_DOCUMENTS	RECEIVE_MMS
REQUEST_COMPANION_RUN_IN_BACKGROUND	READ_VOICEMAIL	READ_EXTERNAL_STORAGE
REQUEST_COMPANION_USE_DATA_IN_BACKGROUND	REQUEST_INSTALL_PACKAGES	WRITE_EXTERNAL_STORAGE
REQUEST_DELETE_PACKAGES	SYSTEM_ALERT_WINDOW	
REQUEST_IGNORE_BATTERY_OPTIMIZATIONS	WRITE_SETTINGS	
SET_ALARM	WRITE_VOICEMAIL	
SET_WALLPAPER		
SET_WALLPAPER_HINTS		
TRANSMIT_IR		
USE_FINGERPRINT		
VIBRATE		
WAKE_LOCK		
WRITE_SYNC_SETTINGS		

Table 2.1: Android permissions and protection levels

Chapter 3

Methods

I conducted this study to explore how undergraduate students enrolled at a private Higher Education Institution in South Africa interacted with Android application security and privacy. To further explore this question, the following research questions were formulated:

1. Do students pay any attention to the application permissions?
   (a) Do the listed permissions deter students from installing the application?
   (b) Do the students pay attention to the permissions declared at run time?
   (c) Do students pay attention to the permissions declared when an application is updated?
2. Do students notice if the application uses encryption and or what encryption is used- do they install applications regardless?
3. Do students notice if the application tracks and publishes their location?

Because this study aimed to take a deeper look at complex user behaviour, a mixed method approach was used. I was interested in the quantitative data

that would show me descriptive statistics of how students interacted with mobile privacy and security. However, the use of qualitative observations and interviews allowed me to gain deeper insights into the quantitative data gathered from my survey. I further used the qualitative data to validate the quantitative data. For example, if the quantitative data derived from the survey indicated that students did not understand mobile permissions, the qualitative data was used to both validate this finding during an observation followed by an interview in order to gain a deeper understanding as to why students did not understand the permissions. This process was chosen in order to gain an holistic view of how students interacted with the mobile privacy and security features.

3.1 Understanding of Permissions and Security

3.1.1 Description of Mobile Applications used

In order to gather the qualitative observation data two custom applications were developed, namely a chat application and a rating application. The chat application (See Figure 3.1) requested permissions one would expect from a chat application, however, the functionality of the application did not match the permissions requested. The application is a text-only chat application which includes no functionality for uploading images, and sharing contacts, voice notes and so forth. The application was published to the Google Play Store and listed as a text only chat application named VCChatter. This application also contained an image of an open lock on the chat screen. This image indicated that the application did not make use of encryption, and was selected from the Android Materials development icons.

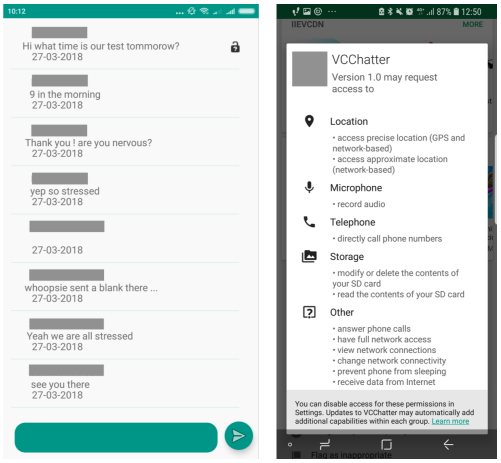


Figure 3.1: Screenshot of the VCChatter app used during interviews and for the survey. This basic text-only app over-requested permissions and was not encrypted.

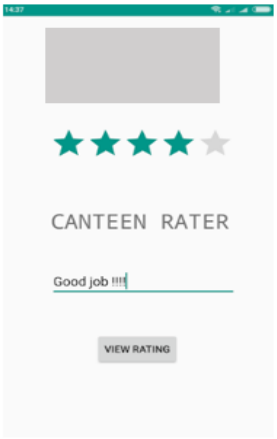


Figure 3.2: Screenshot of the VCCanteenRater app used during interviews and for the survey. This app allowed students to rate the university canteen, and over-requested permissions.

The application lists the following permissions on the Google Play Store:

- Location: Approximate Location.

- Location: Precise Location.
- Phone: Directly Call Phone Numbers.
- Storage: Read Content of USB Storage.
- Storage: Modify or Delete Contents of USB Storage.
- Photos/Media/Files: Read Content of USB Storage.
- Photos/Media/Files: Modify or Delete Contents of USB Storage.
- Microphone: Record Audio.
- Other: Receive Data from the Internet.
- Other: View Network Connections.
- Other: Change Network Connections.
- Other: Full Network Access.
- Other: Prevent Device from Sleeping.

VCCanteenRater (See Figure 3.2) allowed the students to give a star-rating for the university canteen. The application was also over-provisioned and blatantly requested permissions that one would not expect from a rating application. This application simply allowed users to give a rating value and a comment. Although the only permission actually required was network access, the application requested many more permissions than just this.

The application lists the following permissions on the Google Play Store:

- Location: Approximate Location.
- Location: Precise Location.

- Phone: Directly Call Phone Numbers.
- Storage: Read Content of USB Storage.
- Storage: Modify or Delete Contents of USB Storage.
- Photos/Media/Files: Read Content of USB Storage.
- Photos/Media/Files: Modify or Delete Contents of USB Storage.
- Microphone: Record Audio.
- Other: Receive Data from the Internet.
- Other: View Network Connections.

The application types were chosen to both support the deception (see ethical considerations) in the study as well as to support student buy-in. The nature of the application is irrelevant as our study focused on the permissions used by the applications. The institution in question has had requests for an application to rate the on-campus canteen, as well as numerous requests to move to an in-house chat application as many lecturers do not what to join WhatsApp groups as this allows students to contact them personally.

These applications were used in the survey, observations and interviews. Screenshots of the applications as well as the permissions the Google Play Store listed for the applications were used in the survey. Students were asked to install the applications during the observation section and questioned about their behaviour with the applications (often by showing them the permissions allowed or denied for each application on their devices).

Both applications also made use of the institution's logo and colour scheme in order to appear to be representative of the institution. With my applications com-

pleted and ready, I detailed the following process to follow during our observations and interviews.

3.1.2 Types of questions asked

The survey, interview and observation contained many of the same questions. This was intentional to enable me to be able to triangulate the answers given according to what the surveyed students said they did, versus what the students actually did in the observation. The following types of questions were asked:

1. Application installation and use practices.
2. Application update practices.
3. Encryption awareness.
4. Technical ability to find application permission and or encryption information on their devices.
5. Knowledge of the Google Play Store.

3.2 Survey

Simple random sampling was implemented by obtaining (with permission from the institution) a list of the 1,450 students enrolled at the Higher Education Institution. The list was scrambled to ensure that the names were not in alphabetical order, and that students were not listed by qualification. Next, the list was numbered sequentially. An online random number generator was used to randomly generate 150 numbers. 150 students that matched the randomly generated numbers were selected to partake in the study. Students studying towards a degree in

Computer Science were omitted from the study as they study Android development and have a good grasp of how the permissions work.

We targeted 120 responses for the quantitative survey. To ensure that enough responses were collected, the 150 randomly selected students were invited to complete the survey. We contacted the students via telephone and invited them to partake in the study. We made it clear that participation was optional and not mandatory. We e-mailed instructions on how to complete the survey as well as the survey link to each student that agreed to complete the survey. The students were instructed to complete the survey and to either submit the informed consent form on campus, or to e-mail it directly to myself. We used the informed consent form to track responses. I followed up with a WhatsApp message reminder asking the remainder of the students to complete the survey. 130 students responded. Whilst preparing the data for analysis, 27 incomplete responses were removed. The first question of the survey also queried whether the respondents were Android users. The responses of the 26 non-Android users were removed. This left us with 77 completed responses from confirmed Android users. The incomplete responses were removed because we could not explain the reasons candidates had for opting out of completing the survey. They may not have paid attention to the first question and only later discovered that the survey was targeted specifically at Android users. It is possible that the removal of non-Android users could introduce selection bias into the study, however, the wide range of responses and the anonymity of the survey mitigate the effects of selection bias.

The survey enquired about students' mobile installation practices, as well as students' knowledge regarding mobile privacy and security. I asked questions such as "What would prevent you from installing a mobile application ?" I showed them screenshots of mobile permissions listed for applications on the Google Play Store

and enquired if they would install these applications and to provide their reasons for electing to not install the applications.

The survey was designed to include several questions aimed at testing the validity of the student's responses. For example, I presented the students with three questions regarding granting permissions to the custom developed applications. I first showed them the permissions in a list form and not in the familiar Google Play Store setting. I then asked the students to tick each of the listed permissions they would allow for the application. In the very next question, I showed them the actual permissions as listed on the Google Play Store in a screenshot. These permissions were identical to the permissions in the first question. I asked the students if they would install the application, and to give reasons for either installing or not installing the application. The survey questions are included as Appendix 7.1.

3.3 Inclusion of Deception

According to Kelman [Kelman, 1966] deception is introduced into studies because the phenomena that the researcher is attempting to study could be altered if the true nature of the study is known to all participants from the onset. Because I aimed to study the normal behaviour of students, deception was introduced into my study. If I had informed the students that the study explored their perceptions and behaviours with regards to mobile privacy and security, undue attention could have been drawn to these areas.

To counter this phenomenon, the participants were briefed that they were taking part in a usability study for two applications, specifically developed for the institutions' students. The deception was revealed in a written disclosure at the end of the survey or directly following the interview.

Because the inclusion of deception had the potential to cause emotional distress, a campus counsellor was made available to any student who felt the need for one. The students were further informed that they had the option to request that their data be omitted from the study.

3.4 Observation

To gather qualitative data a new sample, which comprised ten percent of the size of the original sample, was used. Ten additional numbers were selected, using random sampling, from the original list, excluding anyone already selected for the initial survey. These students were asked to install two custom developed applications under observation. The students underwent a brief interview directly following the observation.

The students were contacted by telephone and briefed that the institution had developed two custom applications aimed at solving communication problems and improving the services of the on campus canteen. They were further briefed that the institution needed students to test the applications and provide feedback that would be used to improve the applications. Students were also informed that they would be remunerated with a fifty rand voucher from the canteen, and that participation was completely optional. We met the students in a dedicated interview room. Participants were firstly asked to complete the consent form. Next, a research assistant provided the necessary instructions to the participants whilst I observed their actions. An in-depth interview explored the observed behaviours through the use of an interview script. The interviews were conducted directly after the observation.

This protocol was reviewed and accepted by both the University of Cape Town's institutional review board (IRB), as well as the private Higher Education Institu-

tion in question.

3.4.1 Observation Process

We formally greeted all the participants and informed them that they were taking part in a usability study for their campus. Firstly, we introduced the rating application and explained that it would be used by the institution to monitor and improve the on campus canteen's offerings. Thereafter, we introduced the chat application and explained that this application would be used by both students and lecturers to communicate regarding assignments and so forth. Finally, we asked the participants to talk us through their installation procedure. We asked them to explain this to us in a step by step manner, using sentences like: "I am looking for the application on the Play Store", "I have found the application, and I am now downloading it", and "I am beginning the installation".

We observed the students closely as they installed the applications. Special attention was paid to the following:

1. Did the participants look for the full list of application permissions on the Play Store prior to downloading the application?
2. Did the participants pause to read the permissions?
3. Did the participants allow or deny the permissions ?
4. Did the participants allow or deny all the permissions?
5. Did the participants ask any questions regarding the permissions?

We made careful notes of our observations in order to guide our interview process. Thereafter, we conducted interviews of approximately 15 to 30 minutes each, with each participant.

3.5 Interviews

The aim of these interviews was to gain a deeper understanding of the observed behaviour. We designed an interview script that would allow us to ask the necessary questions as well as to dig deeper into the participants' answers. We also kept the script open enough to focus on observed behaviours. We asked similar questions in the interviews, as we did in the survey in order to enable us to compare the survey and interview answers. The deception was revealed midway through the interview after the necessary questions that checked for the students' actual behaviours were asked. These questions were :

1. What did you think about the Canteen Rater / VCChatter ?
2. What would you change about each of the applications?
3. Tell me about your installation experience for both apps, was there anything you saw that was unusual or unexpected? Is there anything you think should be changed?
4. Can you remember which permissions each one of the applications used?

The interview script is included as Appendix 7.1.

3.6 Debriefing and closing of observations and Interviews

A campus counsellor was made available to all participants after the experiment. Any students who experienced emotional distress regarding the deception were directed to the counsellor and had the option to exclude their data from the study.

None of the participants requested the services of the counsellor. Once we gathered and cleaned all the necessary data, I started the data analysis. I detail this process below.

3.7 Data Analysis

3.7.1 Qualitative Data Analysis

According to Hsieh and Shannon [Hsieh and Shannon, 2005] content analysis can be used to describe a process followed by researchers to immerse themselves in the gathered data. Data is then read word for word and coded. The coded data is then interpreted to find any patterns that may emerge.

I used Nvivo to analyse the interview notes to determine if any trends existed. For example: Did most of the students indicate that they paid no attention to Android application permissions because they deemed the application to be safe? I started the analysis with predefined codes:

- I: Ignored Permissions / Security Feature.
- H: Hesitated when faced with Permissions / Security Feature.
- P: Paid attention to Permissions / Security Feature.

The data analysis was repeated until saturation was reached and no further coding could be applied.

3.7.2 Quantitative Data Analysis

I analysed the quantitative data using SciPy and the Pandas Python Suite as the data analysis tool. The findings from the data analysis are presented in descriptive

statistics looking at the percentage of students who paid attention to the security features versus the percentage of students who did not.

3.8 Limitations of the Study

This study only made use of students from a premier private Higher Education Institution. The majority of these students have all attended private schools and can be classed in LSM (Life Style Measurement) seven and eight (middle to higher income brackets). No students from lower LSM brackets or public institutions formed part of the study.

I take cognisance of the work done by Ahmed [Ahmed et al., 2017], as South Africa, in many ways, mimics the governmental control strategies depicted by Ahmed. The Global South is enforcing bio-metric SIM registration while South Africa enforced the RICA (Registration of Interception of Communications) Act. Less developed communities in South Africa also lack identification documents and often share mobile devices [Phokeer et al., 2016]. However, South Africa has a large divide between the rich and the poor, and, in and turn, the ICT services these groups have access to. Molawa [Molawa, 2010] discusses the *first* and *third* world in Africa by describing the differences with regard to first and third world living. Within South Africa exist well developed, first world-like urban areas which are usually populated by affluent South Africans. These South Africans have first world-like access to ICT, international travel and other resources, and do not necessarily match the populations discussed by Ahmed.

It is further possible that participants in the observation were more trusting of the applications because they were led to believe that the applications were being launched by the Higher Education Institution they attended. This possibly could have led students to act in a less secure manner than they normally would have.

I take cognisance of the work done by Nicola Dell on Demand Characteristics [Dell et al., 2012]. Dell goes on to explain that participants in HCI studies often guess the hypothesis of the researcher, and in turn alter their behaviour in support of the researcher's hypothesis. Dell also found that participants are twice as likely to prefer an application if they believe the researcher developed that application. The introduction of deception would mitigate occurrences of Demand Characteristics. The participants in my study believed that they were partaking in a usability study. It is possible that the participants would have favoured the applications more than they usually would have, however, it is unlikely that the participants would have acted more securely even if they had.

This study made use of mainly Millennial participants, who can be defined as individuals born roughly between 1981 and 1996 [Wheeler, 2017] and who are heavily influenced by the technology era. Because of this, the findings of this study could possibly not be extrapolated to the population as a whole. Lastly, there may be occurrences of self-selection bias as I used only 77 of my survey responses, and I cannot account for the security consciousness of the participants who did not respond, or who gave incomplete responses. It is possible that the participants who elected not to participate could have had a very good understanding of mobile privacy and security, and thus could have changed the findings of this study.

Chapter 4

Findings

I discuss my findings according to student understanding of mobile permissions. Because Location-Based Services pose a real risk to students' physical safety, special attention will be paid to this particular permission and it will be discussed as a separate finding. Lastly, I will discuss student interaction with encryption as a security feature. These discussions follow below.

4.1 Understanding of Permissions and Security

4.1.1 Students do not pay attention to application permissions when they install applications.

My findings indicate that only four out of 77 (5%) of the student body pay attention to mobile permissions whilst they install applications. 14 out of 77 (18%) of the surveyed students indicated that they would abort an installation due to discomfort with the permissions requested. Two out of 10 (20%) of the observed students denied the over-provisioned permissions for both applications, and two out of 10

(20%) of the interviewed students listed the permissions of the applications as unusual when asked if they found anything unusual about the applications. When I asked the interview candidates why they did not pay attention to the permissions, they offered the following comments:

> "I never read those permissions, I just click yes, yes, yes." - I10
>
> "Those things are irritating - I just want to get to try the app." - I1
>
> "I never read them, I just click through them. I am excited to see the application." - I3

My findings are different to those of Chin et al [Chin et al., 2012] and Lin et al [Lin et al., 2012] who found that seventeen percent (17%) (Chin) and thirty-five percent (35%) (Alani) of the participants in their studies paid attention to mobile permissions. The large disparity between the findings in my study, and the findings in previous studies can be attributed to changes in the Android APIs. Up until Marshmallow (API 6), applications requested permissions before the installation process. This was changed for Marshmallow, Nougat and more recently Oreo (API 6-8). These APIs request permissions during run time [Android, 2018b]. Since Marshmallow was released in 2015 and is currently used on twenty two percent (22.7%)of smart phones, and Nougat (which was released in 2017) and is used on twenty percent (20.3%) of smart phones [Android, 2018f, Android, 2018d], it is very likely that students have had the most exposure to these API's. The disparity can further be attributed to the fact that my study made use of Millennial participants who are categorised by their need for instant gratification [Teo, 2016] whereas Chin and Alani used a more varied population. The students further displayed a general lack of fear with regards to allowing mobile permissions. When I inquired why they were not worried about installing applications without considering the permissions, many of the students offered the explanation that nothing

had ever happened to them before when they accepted the permissions, and that they doubted whether anything ever would. The students offered comments such as:

"No one is out to get me." - I2

"I always just say yes to those things." - I4

This lack of fear was prevalent throughout my study and elements of it were seen in the survey, interviews and observations. If one considers the fact that malicious applications are often inadvertently installed by mobile users [Khandelwal and Mohapatra, 201 one can argue that unobservant, over-confident digital natives are a cause for concern.

4.1.2 Students do not pay attention to run time permissions - even when they believe they do.

We found a large disparity between what students believe they do and what they actually did. When seeing a list of permissions outside of the Google Play Store environment, an overwhelming number of students indicated that they would not allow the mobile permissions used for our two mobile applications: 49 out of 77 (64%) for the chat application and 55 out of 77 (71%) for the rating application. This changed when we showed them screenshots of the very same application permissions, taken from the Google Play Store. Then, 56 out of 77 (72%) of the students indicated that they would install the chat application, and 40 out of 77 (52%) of the students indicated that they would install the rating application. Of those students who still chose not to install the applications, the permissions were only a factor in 16 out of 77 (20%) for the chat application, and 19 out of 77 (25%) for the rating application. Some of the reasons students provided for not installing the applications were as follows:

"I do not buy food from the canteen." - S5

"I don't think that the application would be useful to me." - S58

"I don't want to chat to my class mates." - S68

Lin, Amini and Hon [Lin et al., 2012] explain that this behaviour could also be attributed to context and expectations. Students expect to see permissions listed in a familiar format on the Play Store and are therefore more likely to allow the permissions. However, if the permissions are shown outside of the familiar context, students are likely to pay more attention.

4.1.3 Students have become desensitised to permissions that are often requested.

An interesting finding that emerged from the data analysis is that nine out of 10 (90%) of the students referred to the dangerous permissions requested by the applications as *standard, default* or *expected* permissions. Some of their responses were as follows:

"Yes, they are the standard permissions that all applications ask for." - I4

"Yes, those are fine – they are the standard permissions." - I10

"They are the standard permissions." - I3

When questioned further it emerged that students trust these permissions because they are requested by most applications they install. Over time, students have become desensitised to these permissions and now believe that these permission requests are safe and harmless. The list of permissions that students described as standard permissions are detailed below:

- Access to Camera
- Access to Microphone: Allows applications to turn the voice recorder on and off.
- Access to Storage: Allows application to read the files stored on the mobile device.
- Access to WiFi: Can turn wireless network on or off and make connections.
- Access to Location: Discloses the physical location of the user using GPS coordinates.
- Access to Phone Calls: Can make and accept phone calls on the mobile device.

This finding can be attributed to the frequent use of these permissions. Hao et al [Hao et al., 2015] found that eighty percent (80%) of the 7737 applications examined in their study used these same permissions. Often these permissions are not necessary for the application to function, but were included by developers to avoid security exceptions. The Android App Permissions Best Practices Guide instructs developers not to use more permissions than needed, and to step back the functionality of their application for those users who elect to deny permissions. For example, an application should still function with limited features if a user elects not to allow access to their contacts [Android, 2018c]. Unfortunately, the open nature of Android markets and the lack of an in-depth evaluation process makes it possible for developers to ignore these best practices [Tan et al., 2015]. Because of the aforementioned, it is possible that these permission requests have lost their efficacy which is unfortunate as these permissions are meant to protect the user's privacy. For example, the Access to External or Internal Storage permissions allow applications to access users' personal files, stored images, photographs, and

so forth. There have been many instances of malicious applications leaking users' data [Tan et al., 2015] and, in turn, negatively affecting their privacy and safety.

4.1.4 Students are not aware that applications make use of more permissions than the explicitly requested permissions.

None of the students were aware that applications make use of more permissions than the dangerous permissions that are explicitly requested. Further to this, none of the students knew how to display the list of full permissions on their devices nor where to look for the permissions used by each application. All the students were unnerved when they were shown the full list of permissions used by each application. They were even more horrified when they were shown the functionality that each permission allows an application on their devices. The students responded with statements such as:

> "No" - I4

> "I seriously did not know that, this is so scary." - I9

> "I had no idea that this is what I have been allowing." - I3

Gerber and Volkamer [Gerber et al., 2015] found similar behaviour in their study. They attributed these findings to the fact that other permissions (as the Play Store refers to protection level normal permissions) are hard to find and not disclosed to users. It would therefore be impossible for novices, or even experienced users who are not developers themselves, to be aware that these permissions exist and are used on their devices. These permissions pose a very real threat to users. For example, the Access and Change WiFi State permissions allow a developer to turn WiFi connections on and off without user intervention [Android, 2018e]. Fang

et al [Fang et al., 2014] further explains that these unknown permissions could stealthily leak users' private data.

4.2 Technical Ability with regards to permissions and privacy

4.2.1 Students do not match the permissions requested to the functionality of the application.

Even students who do pay attention to permissions, do not match the permissions requested to the functionality of the application. None of the interviewed students matched the functionality of the applications to the permissions requested by the application. When this was further queried, most of the students indicated that the idea of matching the permissions the application requests to the actual functionality of the application, is not something they have ever thought about.

From my survey data, I could ascertain that one out of 77 (1%) of the students noticed that the permissions requested by the chat application did not match the functionality of the application. This is interesting, since I clearly stated that the chat application was text-only. Some of their comments were as follows:

> "I would not install the app [sic] as a text only app does not need permission to camera [sic]." - S73

A slightly higher percentage of students, 13 out of 77 (16%), noticed that the rating application was over provisioned. This can be attributed to the fact that the over provisioning of the application is extremely evident. The following comments provide more information on the above:

> "The app doesn't necessarily need any of those permissions to work." - S8

> "I would ask myself why the app would need any of those permissions - and for what reason." - S38

> "An application of this nature should not need access to contacts as well as camera and microphone as it only needs to rate the canteen ." - S40

> "Contents state that it wants me to allow it to read my images in my storage, I do not see how that is important for a canteen rating app." - S76

> "The premissions di [sic] not match what is required of the app. I do not need people to know my location if I just want to look at what is being sold at the canteen." - S28

Liu et al [Liu et al., 2014] attributes similar findings to user's expectations and mental models. They advocate that both these concepts should be included in security evaluations. For example, the students expected a chat application that requested access to a camera, external and internal storage, phone calls, contacts etc, however, they did not expect the same permissions from a rating application. These students have created a mental model [Kang et al., 2015] of what permissions a chat application would require, and the over-provisioning matched both their expectations and mental models, and therefore did not alarm the students. However, the rating application did not match their mental models or expectations [Kang et al., 2015], thus more students noticed the over-provisioning. This clearly indicates that students will pay little attention to the actual functionality

of an application versus the permissions that the application requests if their mental models and expectations are matched. Unfortunately, this finding indicates that students might be vulnerable to well thought out, malicious applications that mimic safe applications.

4.2.2 Students do not know where to check what permissions applications are using.

None of the students knew where on the mobile device to check for the full list of permissions used by applications. Furthermore, none of these students were aware that they needed to expand the settings on their phones to view the full list of permissions used by each application. This finding can also be related to the trust that users place in mobile platforms and developers [Birge, 2009]. Most of the students genuinely believed that they had full control of the applications' permissions because they could toggle these on and off. None of them knew that applications made use of permissions that they had no control over. Kurkovsky [Kurkovsky and Syta, 2010] relates this behaviour to a lack of technical skills. These students might be well versed in social media and instant communication applications [Barak, 2018] however, they lack the technical ability to use their mobile devices safely. They do not know how to secure these devices or how to manage the privacy and security settings of the mobile applications on their devices.

4.2.3 Students do not notice if updates change mobile permissions.

15 out of 77 (33%) of the surveyed students indicated that they considered changes in mobile permissions when they updated mobile applications. In line with this,

one out of 10 (10%) of the observed students indicated that they checked if the permissions changed after an application updated. Unfortunately, and as previously indicated, none of the observed students could successfully show us where on their phones to check the mobile permissions used by each application they installed. This finding can be attributed to the fact that Android-based updates are now largely automatic. According to Android [Android, 2018a], the decision to no longer request permission for updated permissions has been implemented because the user base largely ignored the permissions requested. Android handsets now ship with the Automatic updates over a WiFi feature enabled by default. This setting allows applications to not only install patches or update features, but to also automatically update the dangerous permissions used by the application. A recent XDA article [Developer Admin, 2014] explains the security loophole created by this default setting by stating that a Reddit user was able to automatically update the permissions of his Android app. These updated permissions allowed him to format the storage of any device the application was installed on.

4.3 Student Understanding of Location-Based Services

4.3.1 Students believe they consider location services, however, the data shows that they do not.

When students were shown the Access to Location permission requested by each mobile application in a survey question, 59 out of 77 (77%) of the students indicated that they would not allow this permission for the text only chat app. A further 56 out of 77 (72%) of the students indicated that they would not allow the permission for the rating application. However, in spite of these responses,

56 out of 77 (72%) of the students elected to install the chat application listing the very same permissions they denied. Only 12 out 77 (16%) of the students indicated that they consider location services when installing applications. Li et al [Li and Clark, 2013] had similar findings in their study looking into the attack vectors created by LBS. They found that surprisingly few users paid attention to the applications on their handsets that made use of LBS. Further to this, many of the interviewed students indicated that they were not aware which applications on their mobile phones used LBS, and most of them did not consider the applications that were shipped on their devices.

4.3.2 Students are not sure how location tracking services works.

At least two out of 10 (20%) of the interviewed students indicated that they are not concerned with location services since they never turn them on for too long, or they only use them to check in quickly. None of these students paid attention to the fact their current location would be known regardless of how long they enabled the service for. Some of the comments offered were as follows:

> "I only turn my location on quickly to check in, then I turn it back off." - I1

> "I don't leave it on all the time, only when I am out and about." - I3

Further to this, 31 out of 77 (40%) of the surveyed students indicated that they are not worried about location services because: "No one is out to get them." Li et al [Li and Clark, 2013] supports this finding by stating that users have little understanding around the danger posed by location-based services. Their study found that even regular LBS users believed that their private data was unlikely

to be leaked. Unfortunately their study also found that no exploits were needed to track user locations and display individual identities; the data released by the LBS service was enough to gather the necessary information.

4.4 Understanding of encryption as a security measure

4.4.1 Students do not know what encryption is nor do they recognise encryption symbols.

2 of 10 (20%) of the interviewed students indicated that they knew what encryption was. These students were also only able to provide a very vague explanation of encryption when further questioned. Further to this, the survey respondents provided inconsistent answers when asked, in a single survey question, if they would abort an install based on the lack or presence of encryption. The inconsistency was introduced in two survey questions in order to ensure that my findings were correct (the research questions listed both the presence and lack of encryption as a reason to not install an application). Students acted inconsistently in both questions. See table 5.1.

What would prevent you from installing an app from Varsity College?		
	Y	N
Presence of Encryption	4%	96%
Lack of Encryption	12%	85%

Table 4.1: Students displaying inconsistent encryption related answers

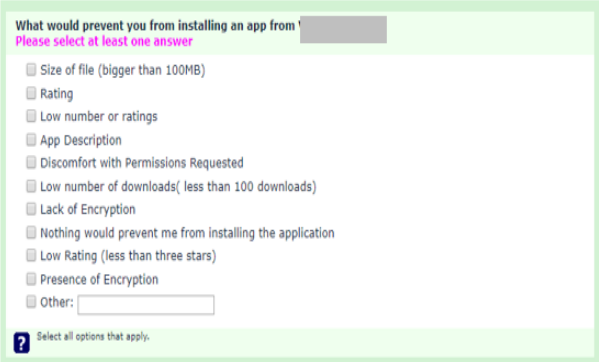


Figure 4.1: Survey question testing both the the presence and lack of encryption.

Mylonas [Mylonas et al., 2013] had similar findings, only twenty-two percent (22%) of his subjects understood or enabled the encryption features on their mobile devices. None of the observed and interviewed students noticed the open lock on the chat application's chat screen. The students tried to click on the lock (see Figure 3.1) when it was pointed out to them. We then asked them what the symbol meant, and the majority of the students indicated that they thought the lock allowed them to private message the contact on which message the lock happened to be. None of the students linked the lock to encryption. This is not a problem unique to South Africa, or even to third world countries. The European Data Protection Supervisor (EDPS) [Supervisor, 2014] states that all mobile applications should use and adequately display the fact that they use encryption. The EDPS goes on to state that users recognise that "https" in the URL in web browsers indicates encryption, however, few mobile applications make use of a consistent symbol to indicate whether encryption is present or not. This finding can be attributed to the fact that students are unaware of the value of their private data. They do not understand that companies reprocess the data they inadvertently supply when they use mobile applications, internet services, and so forth [Santhanam et al., 2017].

Developers should not only indicate if an application is using encryption, but also if the application is not using encryption. It would also be better if a short message is displayed along with an icon, instead of displaying an icon on its own. This will allow digital natives to make an informed decision. The EDPS 2015 guidelines state that more should be done to explicitly show that applications make use of encryption [Supervisor, 2014]. The EDPS further urges developers to make use of encryption, especially for international connections. Developers could also include a short explanation of why encryption is important. See figure 5.4

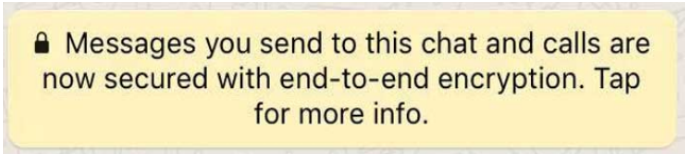


Figure 4.2: Example of WhatsApp using both an encryption icon and a short message to indicated the presence of encryption.

4.5 Overall student competency in terms of mobile permissions, encryption and location-based services

Two out of the surveyed students and one out of the ten interviewed students were consistent and competent in their answers when it came to considering privacy and security. Rashidi et al [Rashidi et al., 2015] found that three percent (3%) of their survey respondents consistently answered the security and privacy questions and could thus be seen as competent. This is an alarmingly small amount of Rashidi et al's and my population which speaks directly to the usability of the Android security and privacy ecosystem. These authors go as far as to recom-

mend a secondary security measure to decide if applications should be placed in a probation setting before they can be deemed as safe.

Chapter 5

Characterising digital natives' approaches to mobile privacy and security

If I compare my findings with those of Kurkovsky, it becomes clear that the security and privacy-related behaviour of digital natives has not changed much. However, the mobile privacy and security landscape has changed drastically and is now much more complex. The amount of mobile applications and, in turn, malicious applications has grown from 38,000 available applications in 2009 to over three million applications in July of 2018 [1]. Popular applications such as Facebook, Twitter, Snapchat and LinkedIn have drastically altered their privacy statements [Yang et al., 2015] and machine learning algorithms now actively use the data we inadvertently supply as we navigate the digital world [Sumner et al., 2012]. If we consider these changes, it becomes evident that a good understanding of how digital natives approach mobile privacy and security is needed to inform security and privacy design decisions. We characterise these approaches below:

[1] https://www.statista.com/statistics/266210/number-of-available-applications-in-the-google-play-store/

https://www.overleaf.com/project/5bb58a0c83c0de09753e7403

5.1 Digital natives lack the necessary technical skills to engage with mobile privacy and security.

Kurkovsky and Syta [Kurkovsky and Syta, 2010] found that digital natives lacked the technical skills to understand and safely use different authentication methods. I can expand on this finding by stating that digital natives lack the technical skills to properly engage with mobile privacy and security as a whole. My findings indicated that digital natives lacked the skills to recognise encryption symbols (see section 4.4.1) with zero out of 10 students recognising the lock icon as an indicator for encryption. None of the students were able to navigate to, and show, the full list of permissions used by the applications installed on their phones (see section 4.2.2). Students were further unable to explain to us how to toggle dangerous permissions on and off, and could not explain how encryption works when asked to do so (see section 4.2.1). It is interesting to note that digital natives' technical skills have not drastically improved, even though mobile breaches and the dangers of non-secure usage of mobile phones have been well reported in the media. It is this lack of skills that keeps this generation from being able to act securely and make informed decisions when they use their mobile phones. It is true that they are well adapted to social media and can be seen as very able in the context of these platforms, however, this generation still has a lot to learn when it comes to the general privacy and security settings made available to them. This current lack of skill leaves them vulnerable to threats such as: identity theft, ransomware, spyware, data leaks, viruses and a wide range of attacks.

Further to this, it becomes clear that mobile applications' privacy and security features needs to be designed for better understanding. We need to create

approaches that will actually be understood by and match the technical ability of digital natives, since our current approaches have clearly failed.

Lastly, it is imperative that Higher Education policymakers and institutions take cognisance of the fact that this generation of students require training specific to mobile privacy and security features.

5.2 Digital natives do not understand mobile and privacy features and therefore ignore them.

My findings indicated that the participants of my study did not understand how mobile security and privacy works: They did not understand the reason for permissions and, in turn, did not pay the necessary attention to the permissions during the installation or use of an application (see sections 4.1.1. 4.1.2). They failed to match the permissions of an application to its functionality, and happily installed over-provisioned applications (see section 4.2.1). They further did not understand what encryption is and why it is important (see section 4.4.1). Lastly, they did not understand how location-based services worked nor that their phone ships with applications that might have LBS enabled (See sections 4.3.1 4.3.2).

These students did not understand the mobile permissions nor the rationales provided for these, and thus elected to ignore these security features all together. Mylonas et al [Mylonas et al., 2013] had similar findings and agrees that users opt to ignore security features that they do not understand, or when they find these overwhelming. They further found that many of the participants in their study did not enable the encryption features available to them. Hanus et al [Hanus and Wu, 2016] explains that users' privacy and security awareness plays a key role in their ability to protect themselves, or to safely use technology. Chanderman and Van Niekerk [Chandarman and Van Niekerk, 2017] echoes these findings

by explaining that better security behaviour is only possible with better security awareness.

Unfortunately my findings showed that the current methods of requesting permissions are not understood and are therefore ineffective.

In order to possibly mitigate the above, the following should be considered:

Permissions should not be requested in permission groups. It is true that Android no longer allows all the permissions in a permission group upon a single permission request [Android, 2018f], however, permissions are still requested in permissions groups, and show only one rationale for all the permissions that exist within that group. For example, an application that requires access to answer phone calls will show the same rationale as an application that requires access to write to your voice mail. Students have no understanding of permission groups and do not even know that they exist. They therefore do not understand that the request they see does not explain exactly what the application will be able to access and can, in fact, be misleading. It may be better to list a rationale for each of the permissions in a group when an application requests only that permission. See table 5.2 and figure 5.1

Android Mobile Permission Group : Phone	
Phone	Read_phone_state
	Read_phone_numbers
	Call_phone
	Answer_phone_calls
	Add_voicemail
	Use_sip

Table 5.1: Android Phone Permission Group

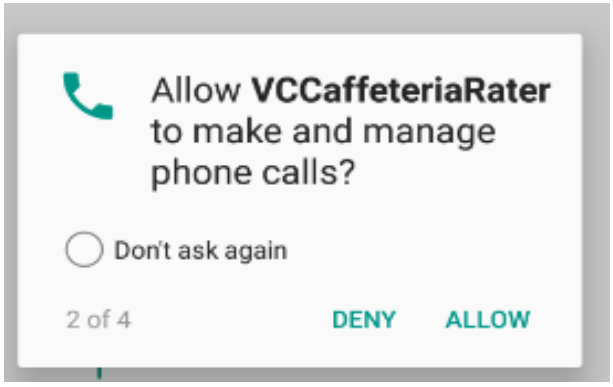


Figure 5.1: Phone Permission Group Rationale.

Digital natives do not understand the full extent of what they are allowing applications access to on their mobile phones. Android and Android developers should use better, more descriptive language in their permission requests. Each request should explain why the permission is necessary, what the permission will do and what will happen if the user elects not to allow the permission. Android does offer permission rationales to partly address this problem, however, the language in the rationales is still not user-friendly enough, and fails to communicate the possible dangers of allowing unnecessary permissions[2]. These rationales are over-simplified and bunch permissions into groups which digital natives do not understand [3].

Lastly, Higher Education Institutions should carefully consider the mobile applications that they prescribe to students. Institutions should take the time to investigate each application in order to ensure that it employs good privacy and security standards.

[2]Android Central. https://www.androidcentral.com/run-permissions-why-change-android-60-may-make-you-repeat-yourself Last Accessed 21 Sept 2018.

5.3 Digital natives have been overexposed to application requests that violate their privacy and have become desensitised.

My findings and those of Harris et al [Harris et al., 2016] indicate that digital natives have become desensitised to mobile permissions (see section 4.1.3). Harris et al focuses on the end users' rationale that they have experienced no adverse effects when installing mobile applications and accepting permissions. My study found that almost the entire list of Android's dangerous permissions are requested so frequently and by so many applications that digital natives now believe that these are a set of standard or default permissions. They see these permissions as a step in the installation process, rather than a security and privacy feature that requires their attention. This has led to permission requests providing little or no security and privacy to digital natives as they allow these permissions by default.

5.4 Digital natives trust the authors of software and fail to act securely when security and privacy features are requested out of context.

The majority of the survey candidates, and nine out of the ten interviewed students believed that Google checks every application that is uploaded to the Play Store (see section 4.1.2). They trust that mobile developers take the time to develop and deliver safe and secure mobile applications that will not leak their data or put them in harms way. This is a fairly concerning characteristic since the Cambridge Analytica [Cadwalladr and Graham-Harrison, 2018] scandal clearly indicated the

consequences of believing that the information you see and share is handled in a safe and secure manner. It is even more concerning if one takes a look at the applications currently available for download on the Google Play Store. Below is a snippet of the various available applications with an almost identical icon to that of Facebook's messenger application - all produced by different authors. Students could inadvertently download the incorrect application and in turn provide unknown parties with valuable and private information. See figures 5.4 and 5.4.

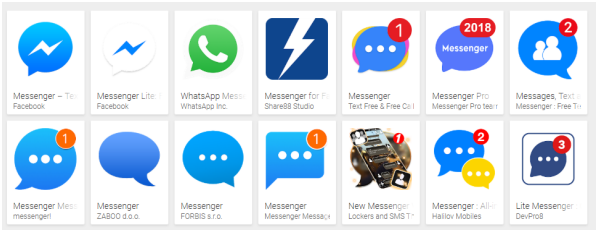


Figure 5.2: Similar Messenger Application Icons with Different Authors on the Google Play Store.

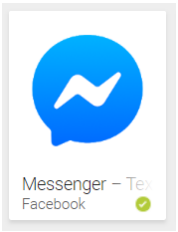


Figure 5.3: Actual Facebook Messenger App.

Students also provided inconsistent responses when they were asked if they would install the custom developed applications in two separate survey questions. One of the questions showed the permissions in text format and the other provided a screenshot of the permissions as listed on the app store (see section 4.1.2). The students did not notice that the permissions were identical and, in fact, for the same application. They were unable to navigate the change in the context in

which the permissions were being displayed. This means that Higher Education Institutions can no longer assume that students will be able to safely navigate mobile application markets and Higher Education policymakers need to consider the fact that the drive for the uptake of technology in Higher Education needs to go hand in hand with policies to ensure that this is done so safely.

5.5 Digital natives' need for instant gratification has consequences for privacy and security.

Santos and Rosati [Santos and Rosati, 2015] argue that the need for immediate gratification is still one of the human race's largest decision biases. Digital natives grew up in a world where instant gratification is not only a possibility, but a standard [Teo, 2016]. My study indicated that their attitude to security is no exception to this rule. Students openly admitted that they would rather just click through the permissions or any other requested security feature to get the gratification of experiencing the application (see section 4.1.1). By doing this, students could have inadvertently installed malicious and possibly dangerous applications on their mobile phones. When students were asked if they would have acted in the same manner if the true nature of the applications were known upfront, almost all of them indicated that they would have acted very differently. They offered comments such as:

> "I would not have installed the application, I see how my actions were not smart." - I3

> "It does not seem worth it now, does it." - I10

Santos and Rosati further state that humans have learned to wait for a better reward or lesser consequences in certain settings, which Fang and Wang [Fang and Wang, 2015]

explain as hyperbolic discounting. They explain that humans are more likely to overlook or withstand instant gratification if the rewards are more long term, however, humans are much more likely to opt for immediate gratification in the short term. Unfortunately, the immediate access and quick turnaround time of application downloads and installations leads to a much higher likelihood of hyperbolic discounting taking place. If we consider the fact that over eighty percent (80%) of the students I observed installed the application with no regard for the permissions, it is clear that hyperbolic discounting does take place (see sections 4.1.1 ,4.1.2, 4.1.3).

Unfortunately the presence of hyperbolic discounting means that any security feature aimed at providing protection to users which is paired with instant gratification will be ineffective.

5.6 Digital natives' definition of privacy is different than those of previous generations.

Both Kurkovsky and Palfrey [Palfrey and Gasser, 2011] explain that digital natives' definition of security is very different from that of the generations that came before them. They happily share their location, photographs, thoughts, music playlists, political beliefs and obvious disdain for Baby Boomers online. Palfrey goes as far as to say that a radical paradigm shift took place and that this generation also has a very different expectation of privacy. It could be possible that this generation's sense of security has eroded [Hoback, 2013] and that they are far easier to exploit than the generations that came before them. Both Kurkosky and Syta [Kurkovsky and Syta, 2010] and myself noted that digital natives displayed *lack of fear* or *carelessness* in their approaches to mobile privacy and security. I now believe that this *lack of fear / carelessness* is, in fact, a manifestation of these

students' eroded definition of privacy.

Higher Education Institutions and policymakers should consider this finding when they prescribe applications to students. The onus lies on the institution to ensure that they prescribe applications that are not over-provisioned and safe to use.

Given the above discussions, it is clear that there is still a lot of research that needs to be done in this area of privacy and security. I conclude my study and discuss some of the possible future works next.

Chapter 6

Conclusions and Future work

Because I was interested in understanding and, in turn, characterising how digital natives interact with mobile privacy and security features, I embarked on a mixed methodology study which employed a survey, an observation and in-depth interviews. I chose this approach because I wanted to explore how students believed they behaved through the survey, and then to contrast these findings according to how the students actually behaved during observations. I followed up the observations with in-depth interviews to gain a deeper understanding as to why students behaved as they did.

I found that: Digital natives lack the necessary technical skills to engage with mobile privacy and security. They do not understand mobile privacy and security features and therefore ignore them. Further to this, digital natives have been overexposed to requests that violate their privacy and have become over desensitised. They trust the authors of software and fail to act securely when security and privacy features are requested out of context. Their instant need for gratification has consequences for privacy and security. Finally, digital natives' definition of privacy is different from that of previous generations.

My findings were similar to those of Kurkovsky and Syta [Kurkovsky and Syta, 2010] who also found that digital natives were not tech-savvy, and in many instances lacked the necessary skills needed to safely use mobile applications. However, my study represents an in-depth look at how South African Higher Education students interacted with mobile privacy and security features by focusing on, in particular, application permissions, encryption and location-based services. I offer a characterisation of their behaviour in order to inform Higher Education Institutions, Higher Education policy and mobile privacy and security designers.

I urge the above mentioned bodies to explore future works into higher education policies. If these policies are going to mandate and drive the use of technology in Higher Education Institutions, they should also mandate and drive that this is done ethically and safely by these institutions.

Higher Education Institutions need to conduct research into – and then design a program tailored to – educating digital natives about safe and secure mobile application usage as well as general safe and secure online behaviour.

Many authors discuss the over-provision of permissions in mobile applications [Mylonas et al., 2013, Imgraben et al., 2014, Khandelwal and Mohapatra, 2015, Liu et al., 2014, Li and Clark, 2013]. This study has clearly indicated that this large-scale over-provisioning has led to digital natives becoming desensitised to mobile permissions. Other authors also state that this has affected the general mobile application population. The real concern here is the power these "standard", "default" or "expected" permissions give mobile applications. A recent Wired magazine article [1] details the fact that Facebook is able to record conversations, travel applications are able to tell when users rotate their phones to view pictures, and Pokemon Go can change anything on your Google Account. These changes are possible due to users grant-

[1] Lauren Goode (2018). App Permissions Don't Tell Us Nearly Enough About Our Apps. Wired, Apr 14, 2018. https://www.wired.com/story/app-permissions/

ing access to Android's dangerous permissions, which they are forced to do, or forego access to the applications and features they want to use. Not only is this over-provisioning reducing the effectiveness of these permissions, it can pose a real security risk to innocent, desensitised, and/or unaware users. If Google is able to track the permissions requested, and features of each app to demand a privacy policy or to assign the correct recommended age restriction per country, surely the system can indicate which applications use all of the dangerous permissions and in turn flag the application as possibly being over-provisioned? The application can then be halted for publishing, until the developer can assure Google that all the requested permissions are, in fact, necessary.

More research should be done in order to find methods to mitigate the effects of the need for instant gratification on privacy and security features.

Lastly, both the Higher Education and development communities need to introduce ethics to developers as soon as possible. Higher Education Institutions that offer computer science and information technology-related degrees need to include a section on ethics. Unfortunately, unethical behaviour in this realm has far reaching consequences which are not always considered.

Bibliography

[Ahmed et al., 2016] Ahmed, S. I., Guha, S., Rifat, M. R., Shezan, F. H., and Dell, N. (2016). Privacy in repair: An analysis of the privacy challenges surrounding broken digital artifacts in bangladesh. In *Proceedings of the Eighth International Conference on Information and Communication Technologies and Development*, page 11. ACM.

[Ahmed et al., 2017] Ahmed, S. I., Haque, M. R., Guha, S., Rifat, M. R., and Dell, N. (2017). Privacy, security, and surveillance in the global south: A study of biometric mobile sim registration in bangladesh. In *Proceedings of the 2017 CHI Conference on Human Factors in Computing Systems*, pages 906–918. ACM.

[Android, 2018a] Android (2018a). Android Security 2017 year in review.

[Android, 2018b] Android (2018b). Developers Guide permissions overview.

[Android, 2018c] Android (2018c). Developers permission best practices.

[Android, 2018d] Android (2018d). Distribution Dashboard platform versions.

[Android, 2018e] Android (2018e). Manifest Permissions change wi-fi sate.

[Android, 2018f] Android (2018f). ReleaseNotes sdk platform release notes.

[Arp et al., 2017] Arp, D., Quiring, E., Wressnegger, C., and Rieck, K. (2017). Privacy threats through ultrasonic side channels on mobile devices. In *Security and Privacy (EuroS&P), 2017 IEEE European Symposium on*, pages 35–47. IEEE.

[Barak, 2018] Barak, M. (2018). Are digital natives open to change? examining flexible thinking and resistance to change. *Computers & Education*, 121:115–123.

[Barn et al., 2014] Barn, B. S., Barn, R., and Tan, J.-P. (2014). Young people and smart phones: An empirical study on information security. In *2014 47th Hawaii International Conference on System Sciences (HICSS)*, pages 4504–4514. IEEE.

[Birge, 2009] Birge, C. (2009). Enhancing research into usable privacy and security. In *Proceedings of the 27th ACM international conference on Design of communication*, pages 221–226. ACM.

[Bullen and Morgan, 2016] Bullen, M. and Morgan, T. (2016). Digital learners not digital natives. *La Cuestión Universitaria*, (7):60–68.

[Cadwalladr and Graham-Harrison, 2018] Cadwalladr, C. and Graham-Harrison, E. (2018). The cambridge analytica files. *The Guardian. Retrieved Mar*, 17:2018.

[Chandarman and Van Niekerk, 2017] Chandarman, R. and Van Niekerk, B. (2017). Students? cybersecurity awareness at a private tertiary educational institution. *The African Journal of Information and Communication*, 2017(20):133–155.

[CHE, 2018] CHE (2018). Counsel for Higher Education review of higher education in south africa.

[Chin et al., 2016] Chin, A. G., Etudo, U., and Harris, M. A. (2016). On mobile device security practices and training efficacy: An empirical study. *Informatics in Education*, 15(2):235.

[Chin et al., 2012] Chin, E., Felt, A. P., Sekar, V., and Wagner, D. (2012). Measuring user confidence in smartphone security and privacy. In *Proceedings of the Eighth Symposium on Usable Privacy and Security*, page 1. ACM.

[Czerniewicz et al., 2006] Czerniewicz, L., Ravjee, N., and Mlitwa, N. (2006). Icts and the south african higher education landscape.

[De Kock and Futcher, 2016] De Kock, R. and Futcher, L. A. (2016). Mobile device usage in higher education institutions in south africa. In *Information Security for South Africa (ISSA), 2016*, pages 27–34. IEEE.

[Dell et al., 2012] Dell, N., Vaidyanathan, V., Medhi, I., Cutrell, E., and Thies, W. (2012). Yours is better!: participant response bias in hci. In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*, pages 1321–1330. ACM.

[Developer Admin, 2014] Developer Admin, X. (2014). XDA 2017 year in review.

[Dhillon et al., 2016] Dhillon, G., Oliveira, T., Susarapu, S., and Caldeira, M. (2016). Deciding between information security and usability: Developing value based objectives. *Computers in Human Behavior*, 61:656–666.

[Du et al., 2017] Du, Y., Wang, J., and Li, Q. (2017). An android malware detection approach using community structures of weighted function call graphs. *IEEE Access*, 5:17478–17486.

[Dunphy et al., 2014] Dunphy, P., Vines, J., Coles-Kemp, L., Clarke, R., Vlachokyriakos, V., Wright, P., McCarthy, J., and Olivier, P. (2014). Understanding

the experience-centeredness of privacy and security technologies. In *Proceedings of the 2014 New Security Paradigms Workshop*, pages 83–94. ACM.

[Fang and Wang, 2015] Fang, H. and Wang, Y. (2015). Estimating dynamic discrete choice models with hyperbolic discounting, with an application to mammography decisions. *International Economic Review*, 56(2):565–596.

[Fang et al., 2014] Fang, Z., Han, W., and Li, Y. (2014). Permission based android security: Issues and countermeasures. *computers & security*, 43:205–218.

[Gerber et al., 2015] Gerber, P., Volkamer, M., and Renaud, K. (2015). Usability versus privacy instead of usable privacy: Google's balancing act between usability and privacy. *ACM SIGCAS Computers and Society*, 45(1):16–21.

[Gkioulos et al., 2017] Gkioulos, V., Wangen, G., Katsikas, S. K., Kavallieratos, G., and Kotzanikolaou, P. (2017). Security awareness of the digital natives. *Information*, 8(2):42.

[Hanus and Wu, 2016] Hanus, B. and Wu, Y. A. (2016). Impact of users' security awareness on desktop security behavior: A protection motivation theory perspective. *Information Systems Management*, 33(1):2–16.

[Hao et al., 2015] Hao, H., Li, Z., and Yu, H. (2015). An effective approach to measuring and assessing the risk of android application. In *Theoretical Aspects of Software Engineering (TASE), 2015 International Symposium on*, pages 31–38. IEEE.

[Harris et al., 2016] Harris, M. A., Brookshire, R., and Chin, A. G. (2016). Identifying factors influencing consumers' intent to install mobile applications. *International Journal of Information Management*, 36(3):441–450.

[Hoback, 2013] Hoback, C. (2013). *Terms and Conditions May Apply*. iMDB.

[Hsieh and Shannon, 2005] Hsieh, H.-F. and Shannon, S. E. (2005). Three approaches to qualitative content analysis. *Qualitative health research*, 15(9):1277–1288.

[Imgraben et al., 2014] Imgraben, J., Engelbrecht, A., and Choo, K.-K. R. (2014). Always connected, but are smart mobile users getting more security savvy? a survey of smart mobile device users. *Behaviour & Information Technology*, 33(12):1347–1360.

[Jaffer et al., 2007] Jaffer, S., Ng'ambi, D., and Czerniewicz, L. (2007). The role of icts in higher education in south africa: One strategy for addressing teaching and learning challenges. *International journal of Education and Development using ICT*, 3(4):131–142.

[Johnson et al., 2012] Johnson, R., Wang, Z., Gagnon, C., and Stavrou, A. (2012). Analysis of android applications' permissions. In *Software Security and Reliability Companion (SERE-C), 2012 IEEE Sixth International Conference on*, pages 45–46. IEEE.

[Kang et al., 2015] Kang, R., Dabbish, L., Fruchter, N., and Kiesler, S. (2015). my data just goes everywhere:" user mental models of the internet and implications for privacy and security. In *Symposium on Usable Privacy and Security (SOUPS)*, pages 39–52. USENIX Association Berkeley, CA.

[Kelley et al., 2012] Kelley, P. G., Consolvo, S., Cranor, L. F., Jung, J., Sadeh, N., and Wetherall, D. (2012). A conundrum of permissions: installing applications on an android smartphone. In *International Conference on Financial Cryptography and Data Security*, pages 68–79. Springer.

[Kelman, 1966] Kelman, H. C. (1966). Deception in social research. *Trans-action*, 3(5):20–24.

[Khandelwal and Mohapatra, 2015] Khandelwal, A. and Mohapatra, A. (2015). An insight into the security issues and their solutions for android phones. In *Computing for Sustainable Global Development (INDIACom), 2015 2nd International Conference on*, pages 106–109. IEEE.

[Kurkovsky and Syta, 2010] Kurkovsky, S. and Syta, E. (2010). Digital natives and mobile phones: A survey of practices and attitudes about privacy and security. In *Technology and Society (ISTAS), 2010 IEEE International Symposium on*, pages 441–449. IEEE.

[Li et al., 2006] Li, M., Sampigethaya, K., Huang, L., and Poovendran, R. (2006). Swing & swap: user-centric approaches towards maximizing location privacy. In *Proceedings of the 5th ACM workshop on Privacy in electronic society*, pages 19–28. ACM.

[Li and Clark, 2013] Li, Q. and Clark, G. (2013). Mobile security: a look ahead. *IEEE Security & Privacy*, 11(1):78–81.

[Lin et al., 2012] Lin, J., Amini, S., Hong, J. I., Sadeh, N., Lindqvist, J., and Zhang, J. (2012). Expectation and purpose: understanding users' mental models of mobile app privacy through crowdsourcing. In *Proceedings of the 2012 ACM Conference on Ubiquitous Computing*, pages 501–510. ACM.

[Liu et al., 2014] Liu, B., Lin, J., and Sadeh, N. (2014). Reconciling mobile app privacy and usability on smartphones: Could user privacy profiles help? In *Proceedings of the 23rd international conference on World wide web*, pages 201–212. ACM.

[Miller et al., 2012] Miller, K. W., Voas, J., and Hurlburt, G. F. (2012). Byod: Security and privacy considerations. *It Professional*, 14(5):53–55.

[Molawa, 2010] Molawa, S. (2010). The "first" and "third world" in africa: knowledge access, challenges and current technological innovations in africa.

[Mtega et al., 2012] Mtega, W. P., Bernard, R., Msungu, A. C., and Sanare, R. (2012). Using mobile phones for teaching and learning purposes in higher learning institutions: The case of sokoine university of agriculture in tanzania.

[Mylonas et al., 2013] Mylonas, A., Kastania, A., and Gritzalis, D. (2013). Delegate the smartphone user? security awareness in smartphone platforms. *Computers & Security*, 34:47–66.

[Ongtang et al., 2010] Ongtang, M., Butler, K., and McDaniel, P. (2010). Porscha: Policy oriented secure content handling in android. In *Proceedings of the 26th Annual Computer Security Applications Conference*, pages 221–230. ACM.

[Palfrey and Gasser, 2011] Palfrey, J. G. and Gasser, U. (2011). *Born digital: Understanding the first generation of digital natives*. ReadHowYouWant. com.

[Phokeer et al., 2016] Phokeer, A., Densmore, M., Johnson, D., and Feamster, N. (2016). A first look at mobile internet use in township communities in south africa. In *Proceedings of the 7th Annual Symposium on Computing for Development*, page 15. ACM.

[Porter et al., 2014] Porter, W. W., Graham, C. R., Spring, K. A., and Welch, K. R. (2014). Blended learning in higher education: Institutional adoption and implementation. *Computers & Education*, 75:185–195.

[Quay-de la Vallee et al., 2016] Quay-de la Vallee, H., Selby, P., and Krishnamurthi, S. (2016). On a (per) mission: Building privacy into the app marketplace. In *Proceedings of the 6th Workshop on Security and Privacy in Smartphones and Mobile Devices*, pages 63–72. ACM.

[Rambe and Bere, 2013] Rambe, P. and Bere, A. (2013). Using mobile instant messaging to leverage learner participation and transform pedagogy at a s outh a frican u niversity of t echnology. *British Journal of Educational Technology*, 44(4):544–561.

[Rao and Girme, 2015] Rao, U. P. and Girme, H. (2015). A novel framework for privacy preserving in location based services. In *Advanced Computing & Communication Technologies (ACCT), 2015 Fifth International Conference on*, pages 272–277. IEEE.

[Rashidi et al., 2015] Rashidi, B., Fung, C., and Vu, T. (2015). Dude, ask the experts!: Android resource access permission recommendation with recdroid. In *Integrated Network Management (IM), 2015 IFIP/IEEE International Symposium on*, pages 296–304. IEEE.

[Ruxwana and Msibi, 2018] Ruxwana, N. and Msibi, M. (2018). A south african university's readiness assessment for bringing your own device for teaching and learning. *South African Journal of Information Management*, 20(1):1–6.

[Santhanam et al., 2017] Santhanam, G. R., Holland, B., Kothari, S., and Mathews, J. (2017). Interactive visualization toolbox to detect sophisticated android malware. In *Visualization for Cyber Security (VizSec), 2017 IEEE Symposium on*, pages 1–8. IEEE.

[Santos and Rosati, 2015] Santos, L. R. and Rosati, A. G. (2015). The evolutionary roots of human decision making. *Annual review of psychology*, 66:321–347.

[Sarma et al., 2012] Sarma, B. P., Li, N., Gates, C., Potharaju, R., Nita-Rotaru, C., and Molloy, I. (2012). Android permissions: a perspective combining risks and benefits. In *Proceedings of the 17th ACM symposium on Access Control Models and Technologies*, pages 13–22. ACM.

[Singh et al., 2016] Singh, P., Singh, S., and Tiwari, P. (2016). Discovering persuaded risk of permission in android applications for malicious application detection. In *Inventive Computation Technologies (ICICT), International Conference on*, volume 3, pages 1–5. IEEE.

[Sumner et al., 2012] Sumner, C., Byers, A., Boochever, R., and Park, G. J. (2012). Predicting dark triad personality traits from twitter usage and a linguistic analysis of tweets. In *Machine learning and applications (icmla), 2012 11th international conference on*, volume 2, pages 386–393. IEEE.

[Supervisor, 2014] Supervisor, E. D. P. (2014). EDPS guidelines on the protection of personal data processed by mobile applications.

[Tan et al., 2015] Tan, D. J., Chua, T.-W., Thing, V. L., et al. (2015). Securing android: a survey, taxonomy, and challenges. *ACM Computing Surveys (CSUR)*, 47(4):58.

[Tang et al., 2017] Tang, J., Li, R., Han, H., Zhang, H., and Gu, X. (2017). Detecting permission over-claim of android applications with static and semantic analysis approach. In *Trustcom/BigDataSE/ICESS, 2017 IEEE*, pages 706–713. IEEE.

[Teo, 2016] Teo, T. (2016). Do digital natives differ by computer self-efficacy and experience? an empirical study. *Interactive Learning Environments*, 24(7):1725–1739.

[Wang et al., 2017] Wang, Y., Rawal, B., Duan, Q., and Zhang, P. (2017). Usability and security go together: A case study on database. In *Recent Trends and Challenges in Computational Models (ICRTCCM), 2017 Second International Conference on*, pages 49–54. IEEE.

[Wheeler, 2017] Wheeler, S. A. (2017). Thriving millennials: The next generation of industry professionals. *The Journal of Equipment Lease Financing (Online)*, 35(3):1–6.

[Yang et al., 2015] Yang, R., Ng, Y. J., and Vishwanath, A. (2015). Do social media privacy policies matter? evaluating the effects of familiarity and privacy seals on cognitive processing. In *System Sciences (HICSS), 2015 48th Hawaii International Conference on*, pages 3463–3472. IEEE.

[Zhu et al., 2013] Zhu, J., Kim, K.-H., Mohapatra, P., and Congdon, P. (2013). An adaptive privacy-preserving scheme for location tracking of a mobile user. In *Sensor, Mesh and Ad Hoc Communications and Networks (SECON), 2013 10th Annual IEEE Communications Society Conference on*, pages 140–148. IEEE.

6.1 Appendixes

6.1.1 Survey

Exploring the usability of custom developed applications for Varsity College Durban North.

This questionaire is aimed to better understand your use of Android based mobile phone applications.
Thank you for taking the time to complete my survey. Kindly answer ALL the questions in the survey as truthfully as you can.

There are 19 questions in this survey

Usability of Android Applications

[]Do you use an Android mobile (cell) phone?

Please choose **only one** of the following:

- ○ Yes
- ○ No

If the answer to this question is NO, please do not complete this survey.

[]

How often do you download and install new applications?

Please choose **only one** of the following:

- ○ Daily
- ○ Weekly
- ○ Monthly
- ○ Never
- ○ Yearly
- ○ Other

[]What would prevent you from installing an app from Varsity College?

Please select at least one answer

Please choose **all** that apply:

- ☐ Size of file (bigger than 100MB)
- ☐ Rating
- ☐ Low number or ratings
- ☐ App Description
- ☐ Discomfort with Permissions Requested
- ☐ Low number of downloads(less than 100 downloads)
- ☐

Lack of Encryption

- [ ] Nothing would prevent me from installing the application
- [ ] Low Rating (less than three stars)
- [ ] Presence of Encryption
- [ ] Other:

Select all options that apply.

[]What do you consider when choosing applications to install

Please select at least one answer

Please choose **all** that apply:

- [ ] Size of file (bigger than 100MB)
- [ ] Rating (less than three stars)
- [ ] Low number of Ratings
- [ ] App Description
- [ ] Available space on phone
- [ ] Low Number of Downloads (less that 100 downloads)
- [ ] Lack of Encryption
- [ ] Access To location services
- [ ] Presence of Encryption
- [ ] I do not really consider anything, I just download the app
- [ ] Other:

Select all options that apply.

[]Describe the steps you follow when you download and install an application.

Please write your answer here:

Explain from the very beginning , for example from when you access the playstore.

[]Which of the following mobile applications do you use at least once a week?

Please select at least one answer

Please choose **all** that apply:

- [ ] FaceBook
- [ ] Twitter
- [ ] SnapChat
- [ ] Instagram
- [ ] Gmail
- [ ] Netflix
- [ ] Showmax
- [ ] Other:

Please select all that apply

[]Can you list the application permissions used by the applcation that you selected in the previous question?

Please choose **only one** of the following:

- ○ Yes
- ○ No

You are welcome to use your phone to look for the permissions.

[]Rank the following mobile permissions in order of how potentially harmful they may be?(Please rank from most harmful to least harmful)

All your answers must be different.

Please number each box in order of preference from 1 to 10

- [ ] Access to External Storage
- [ ] Access to Location
- [ ] Access to contacts
- [ ] Access to SMS
- [ ] Access to Camera
- [ ] Access to Images
- [ ] Access to Calls
- [ ] In App purchases
- [ ] Access to Wifi

☐ Change Network State

Rank in order from Most dangerous to least dangerous.

[]Can you explain what the Access to External Storage permissions allows an application to do on your phone?

Please write your answer here:

[]Which of the following applications do you believe make use of encryption?

Please select at least one answer

Please choose **all** that apply:

- ☐ Facebook
- ☐ WhatsApp
- ☐ YouTube
- ☐ Absa Banking
- ☐ Candy Crush
- ☐ Twitter

Please select all options that apply.

[] Do you know which applications currently installed on your phone make use of location services?

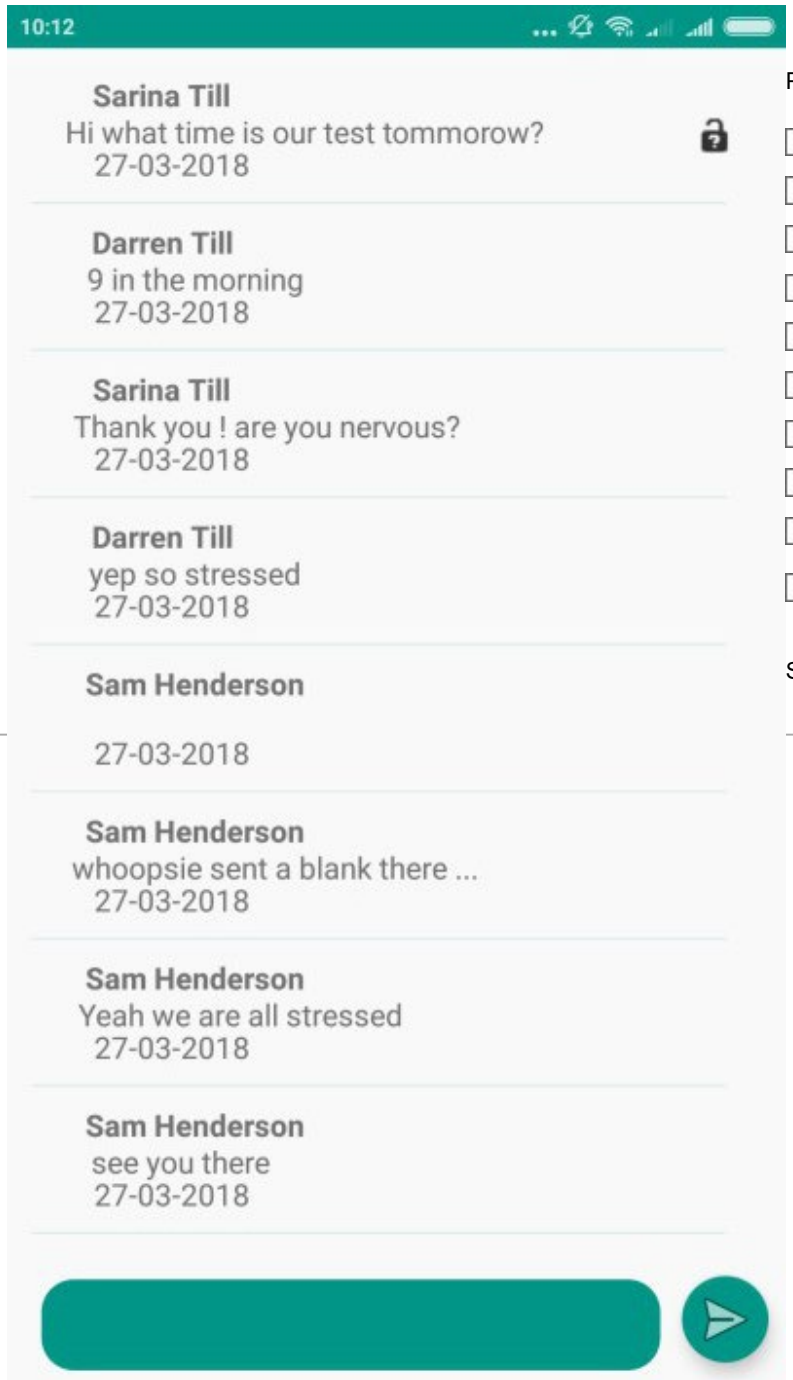
Please choose **only one** of the following:

- ○ Yes
- ○ No

[]

Consider the text only chat application below:

Out of the permissions listed below, which permissions would you allow for this application?



Please choose **all** that apply:

- [ ] Access to Camera
- [ ] Access to Location
- [ ] Access to Contacts
- [ ] Access to Internal Storage
- [ ] Access to External Storage
- [ ] Access to Wifi
- [ ] Access to Phone Calls
- [ ] Access to Network
- [ ] None of the above
- [ ] Other:

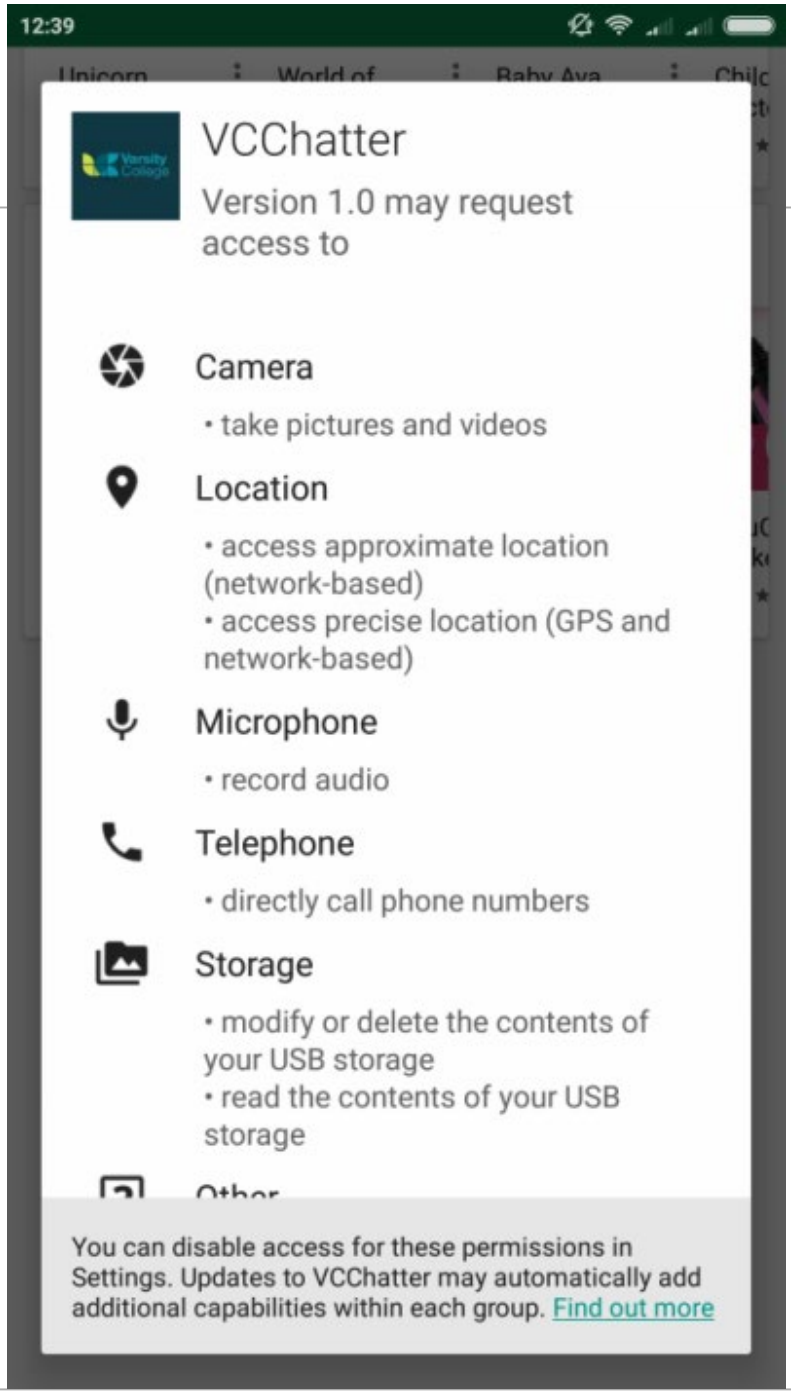
Select all options that apply.

[]

Below are the permissions listed for the applcation. Would you install this application?

Please choose **only one** of the following:

- ○ Yes
- ○ No



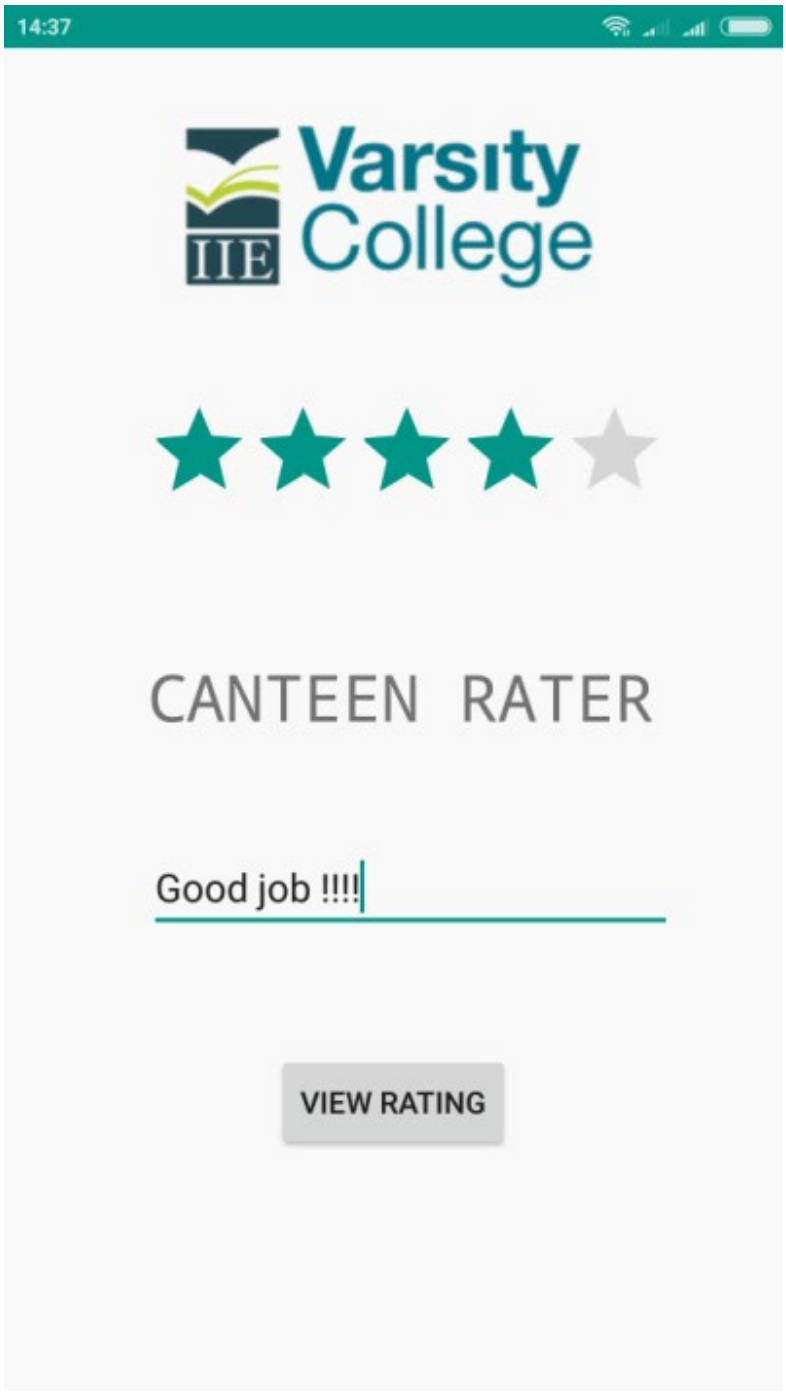
[]Briefly explain your reasons for installing or NOT installing the appliaction from the previous question.

Please write your answer here:

[]

Consider the application below:

Which permissions would you allow for this application?



Please choose **all** that apply:

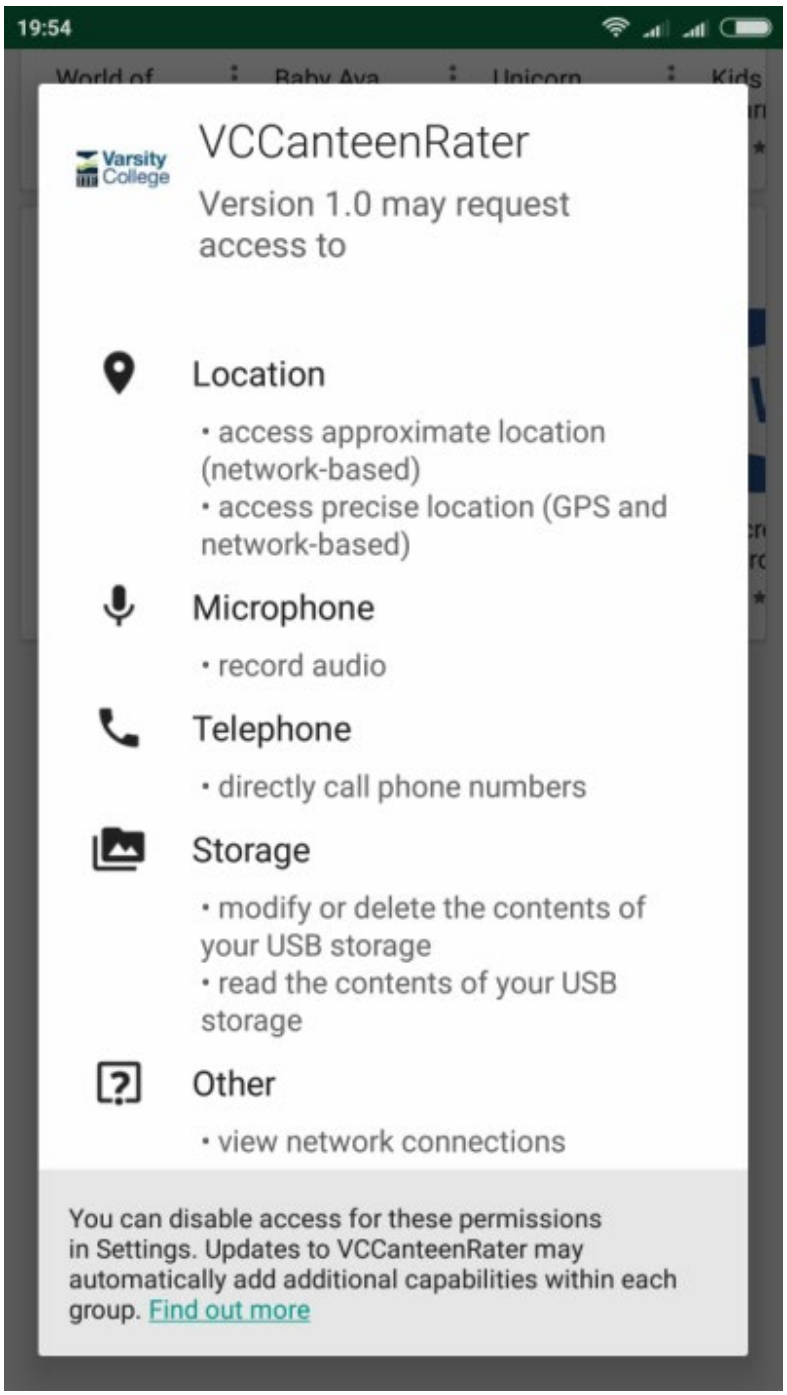
- [ ] Access to Camera

- [ ] Access to Location
- [ ] Access to Contacts
- [ ] Access to Internal Storage
- [ ] Access to External Storage
- [ ] Access to Network State
- [ ] None of the Above
- [ ] Other:

Select all that apply.

[]

These are the permissions used by the application, would you install this application?



Please choose **only one** of the following:

- ○ Yes
- ○ No

[]Briefly explain your reasons for why you would /would NOT install this application.

Please write your answer here:

[]Which of the following do you take into consideration when applications are updated?

Please choose **all** that apply:

- ☐ WIFI Access
- ☐ The size of the download
- ☐ New Features included
- ☐ Updated Permissions
- ☐ Bug fixes
- ☐ Security Patches
- ☐ Other:

Select all options that apply.

[]

Do you believe all applications are checked by Google before they are released on the PlayStore?

Please choose **only one** of the following:

- ○ Yes
- ○ No

Thank you for completing my survey,

You were led to believe that this study explores the usability of custom developed applications for Varsity College. In truth the study actually explored under graduate perseptions and interaction with Android mobile applications privacy and security.

Deception was introduced into the study to ensure that candidates answer as they normally would and not pay undue attention to the privacy and security features.

Should want to discuss this matter further or withdraw your data from the study, you are welcome to contact me at ctill@varsitycollege.co.za

Submit your survey.
Thank you for completing this survey.

6.1.2 Interview Script

1. General

   (a) What did you think of CanteenRater?

   (b) What did you think of VCChatter?

   (c) What would you change about either of the two apps?

   (d) Tell me about your installation experience for both app, was there anything you saw that was unusual or unexpected? Is there anything you think should be changed?

   (e) What does each app do?

   (f) Can you remember which permissions each one of the applications used?

   (g) (Display the actual permissions to the participant.) Do you think each these permissions are necessary?

   (h) Would you have installed both apps with the current permissions if you did not recognize the publisher?

   (i) What If you did not recognize the publisher but all your friends were using it?

   (j) What do you think are some security risks entailed in using each application?

   (k) What permissions would you allow?

2. Application Permissions:

   (a) Tell me what you understand about Android App (Application) Permissions?

   (b) Do you believe that all applications published in the play store have been tested and approved by Google?

(c) I noticed that you did not pay any attention to the permissions whilst installing, please explain why / I noticed that you paid attention to the permissions whilst installing, please explain why.

(d) Tell me about the last time you recall installing or updated an app that required additional permissions.

(e) Please list the permissions that you allowed, and what you thought about each one.

(f) Have you ever decided not to install on a mobile application based on the permissions?

(g) If you answered yes ,please elaborate?

(h) Have you ever felt uncomfortable with or unclear about what permissions were being requested, and installed the application anyways? If so, tell me about it – what was uncomfortable or unclear and why did you choose.

3. Updates:

(a) I noticed you installed / did not install based on the update permissions – please explain your thinking?

(b) Have you ever updated an application even though it added extreme permissions and why?

4. Location Publishing:

(a) Are you currently aware if any application installed on the phone actively publishes your location?

(b) If you answered yes , list the applications that publishes your location ?

(c) Do you believe it is dangerous to have your location published?

(d) If you answered yes to both previous questions, can you explain why you still make use of applications that publish your location?

(e) Is it possible to check which applications publish your location after you have installed them?

(f) Can you show me where on your device to check?

5. Encryption

(a) Tell me about your understanding of encryption?

(b) Do you enquire if any of the applications you install make use of encryption?

(c) If you have answered No to the previous question , can you explain why you do not inquire if applications make use of encryption?

(d) If you have answered Yes t, how often do you inquire if an application makes use of encryption?

(e) Do you believe it is important to make use of encryption when using mobile phones for communication? Elaborate on your answer.

6.1.3 Informed Consent Form

DEPARTMENT OF COMPUTER SCIENCE

UNIVERSITY OF CAPE TOWN
PRIVATE BAG X3
RONDEBOSCH 7701
SOUTH AFRICA

RESEARCHER: Sarina Till
TELEPHONE: +27-31-762 3010
FACSIMILE: +27-31-762 3010
E-MAIL: ctill@varsitycollege.co.za
URL: www.cs.uct.ac.za

Informed Voluntary Consent to Participate in Research Study

Project Title: Usability study for institute specific , custom developed Android based mobile applications.

Invitation to participate, and benefits: You are invited to participate in a research study conducted with undergraduate students. The study aim is to conduct a usability study on two mobile applications designed for use by Varsity College. I believe that your experience would be a valuable source of information, and hope that by participating you may gain useful knowledge.

Procedures: During this study, you will be asked to partake in a usability study and/or complete a survey. Should you be selected for the usability study, you will be asked to install two mobile applications under observation. A short interview regarding the usability and over all experience of the applications will be conducted directly after the experiment.

Risks: There is a very small risk of emotional discomfort.

Disclaimer/Withdrawal: Your participation is completely voluntary; you may refuse to participate, and you may withdraw at any time without having to state a reason and without any prejudice or penalty against you. Should you choose to withdraw, the researcher commits not to use any of the information you have provided without your signed consent. Note that the researcher may also withdraw you from the study at any time.

Confidentiality: All information collected in this study will be kept private in that you will not be identified by name or by affiliation to an institution. Confidentiality and anonymity will be maintained as pseudonyms will be used.

What signing this form means:

By signing this consent form, you agree to participate in this research study. The aim, procedures to be used, as well as the potential risks and benefits of your participation have been explained verbally to you in detail, using this form. Refusal to participate in or withdrawal from this study at any time will have no effect on you in any way. You are free to contact me, to ask questions or request further information, at any time during this research.

I agree to participate in this research (tick one box)

☐ **Yes** ☐ No _M.M._____ (Initials)

Matthew Meyer	M.M	5 April 2018
Name of Participant	Signature of Participant	Date

Name of Researcher	Signature of Researcher	Date